NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA

THESIS

EFFECTS OF DIGITAL AVIONICS SYSTEMS ON THE SURVIVABILITY OF MODERN TACTICAL AIRCRAFT

by

Wade D. Duym

June 1995

Thesis Advisor: Robert E. Ball

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)

2. REPORT DATE June 1995

3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE EFFECTS OF DIGITAL AVIONICS SYSTEMS ON THE SURVIVABILITY OF MODERN TACTICAL AIRCRAFT

5. FUNDING NUMBERS

6. AUTHOR(S) Duym, Wade D.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

Many modern tactical aircraft incorporate digital avonics systems with federated, centralized or distributed avionics architectures that share data via interconnecting data buses. The design of a digital avionics architecture has an impact on the combat survivability of the aircraft. Survivability in combat is defined as "the capability of the aircraft to avoid and/or withstand a man-made hostile environment." Survivability is made up of two elements; 1) susceptibility, the inability of the aircraft to avoid being damaged by the various elements of the man-made hostile environment, and 2) vulnerability, the ability of the aircraft to withstand the damage caused by the hostile environment. Thus, a tactical aircraft should be designed to avoid being hit and to survive if hit. This thesis explores the survivability advantages and disadvantages inherent in the design of digital avionics system architectures.

14. SUBJECT TERMS Avionics, Survivability, Vulnerability, Susceptibility, Vulnerability Assessment, Data Bus

15. NUMBER OF PAGES 80

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified

18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified

19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified

20. LIMITATION OF ABSTRACT UL

Approved for public release; distribution is unlimited.

EFFECTS OF DIGITAL AVIONICS SYSTEMS
ON THE SURVIVABILITY
OF MODERN TACTICAL AIRCRAFT

Wade D. Duym
Commander, United States Navy
B.A., Muskingum College, 1974
M.S., Naval Postgraduate School, 1982

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ENGINEERING SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
June 1995

Author: ______________________________
Wade D. Duym

Approved by: Robt E Ball
Robert E. Ball, Thesis Advisor

I Kaminer
Issac I. Kaminer, Second Reader

Daniel J Collins
Daniel J. Collins, Chairman
Department of Aeronautics and Astronautics

ABSTRACT

Many modern tactical aircraft incorporate digital avonics systems with federated, centralized or distributed avionics architectures that share data via interconnecting data buses. The design of a digital avionics architecture has an impact on the combat survivability of the aircraft. Survivability in combat is defined as "the capability of the aircraft to avoid and/or withstand a man-made hostile environment." Survivability is made up of two elements; 1) susceptibility, the inability of the aircraft to avoid being damaged by the various elements of the man-made hostile environment, and 2) vulnerability, the ability of the aircraft to withstand the damage caused by the hostile environment. Thus, a tactical aircraft should be designed to avoid being hit and to survive if hit. This thesis explores the survivability advantages and disadvantages inherent in the design of digital avionics system architectures.

TABLE OF CONTENTS

I. INTRODUCTION 1

A. AVIONICS 1

B. SURVIVABILITY 2

C. SURVIVABILITY ASSESSMENT 4

D. THESIS ORGANIZATION 5

II. DIGITAL AVIONICS SYSTEMS BACKGROUND 7

A. DIGITAL AVIONICS 7

B. DIGITAL AVIONICS ARCHITECTURES 8

C. AIRCRAFT ELECTRICAL POWER 11

D. AVIONICS DATA BUSES 12

1. Military Aircraft 12

2. Civil Aircraft 14

E. MICROPROCESSORS 15

F. SENSORS 17

G. AVIONICS DISPLAYS 17

III. SUSCEPTIBILITY EFFECTS 19

A. SUSCEPTIBILITY 19

B. THREAT WARNING 20

C. NOISE JAMMING AND DECEIVING 20

D. SIGNATURE REDUCTION 21

E. EXPENDABLES 22

F. THREAT SUPPRESSION 22

G. TACTICS 23

IV. VULNERABILITY EFFECTS 25

A. VULNERABILITY 25

B. KILL CATEGORIES 25

C. DAMAGE MECHANISMS AND DAMAGE PROCESSES 26

D. VULNERABILITY ASSESSMENT 27

E. CRITICAL COMPONENTS 29

F. LOSS OF FLIGHT CONTROL (ATTRITION) KILL . . . 32
G. LOSS OF ENGINE CONTROL SYSTEMS (MISSION ABORT) KILL 37
H. LOSS OF FLIGHT AVIONICS (MISSION ABORT) KILL . 38
I. LOSS OF TACTICAL SENSOR SYSTEMS (MISSION ABORT) KILL 40
J. ARCHITECTURES 43
1. Federated 43
2. Centralized 44
3. Distributed 46

V. COMPUTING THE VULNERABLE AREA OF AVIONICS COMPONENTS 49
A. VULNERABILITY ASSESSMENT 49
B. "BLACK BOX" VULNERABILITY 51
C. CABLE VULNERABILITY 54

VI. VULNERABILITY REDUCTION IN AVIONICS DESIGN 57
A. VULNERABILITY REDUCTION CONCEPTS 57
1. Component Redundancy (With Separation) . 58
2. Component Location 58
3. Passive Damage Suppression 59
4. Active Damage Suppression 60
5. Component Shielding 60
6. Component Elimination 61
B. CHOICE OF AVIONICS ARCHITECTURE 61
1. Federated 61
2. Centralized 62
3. Distributed 62

VII. CONCLUSIONS 63

LIST OF REFERENCES 65

INITIAL DISTRIBUTION LIST 69

I. INTRODUCTION

A. AVIONICS

Electronic devices and systems that are used in aircraft are commonly referred to as **avionics**. Typical systems within the general class of avionics systems include [Ref. 1: p. 1]:

- Flight control systems (e.g. fly-by-wire controls, autopilot).
- Engine control systems (e.g. Full Authority Digital Electronic Controls (FADEC)).
- Flight avionics systems (e.g. communications, navigation, flight instruments).
- Tactical sensor systems, both passive and active (e.g. radar, electro-optical and electronic warfare).
- Computer systems.

Avionics systems are generally divided between analog and digital types, depending on the manner in which the electronic signal is represented. Older analog avionics systems have largely been replaced by the digital avionics systems that are used in most modern tactical aircraft. These digital avionics systems are characterized by:

- Widespread use of **microprocessors** for computation
- Electronic **sensors** using digital signal processing
- Programmable **displays** such as cathode ray tubes or liquid crystal displays
- Extensive use of high speed **digital data buses.**

There are many design and performance advantages of digital avionics architectures, including: reduced weight, improved reliability, increased performance, reduced component count, sensor data sharing/sensor fusion, etc. However, the cost of the digital avionics can be high; in modern tactical aircraft the avionics cost is approximately 30-50% of the total aircraft fly-away cost [Ref. 2]. Because of the high cost of modern tactical aircraft, as well as for many other good reasons, tactical aircraft must be survivable if they are to be effective.

B. SURVIVABILITY

A tactical aircraft must be designed with the hostile environment of combat in mind so that the aircraft can survive to complete its mission and return to base. More efficient and capable tactical aircraft should also be more survivable in a hostile environment. Survivability in combat is defined as "the capability of an aircraft to avoid and/or withstand a man-made hostile environment" [Ref. 3: p. 1]. A tactical aircraft should be designed to avoid being hit, and to survive if hit. Survivability is made up of two elements: susceptibility, the inability of the aircraft to avoid being damaged by the various elements of the man-made hostile environment [Ref. 3: p.223]; and vulnerability, the inability of the aircraft to withstand the damage caused by the man-made hostile environment [Ref. 3: p. 135].

The susceptibility of an aircraft is influenced by the aircraft's design, the tactics that are used and the survivability equipment and weapons that it carries. Aircraft designed for combat environments generally incorporate features designed to reduce the likelihood of detection by hostile forces and features designed to reduce the probability of being hit, if detected. One such susceptibility reduction feature is "stealth", which includes signature reduction techniques applicable to the aircraft's radar, infrared, visual and acoustic signatures. The use of appropriate tactics is also important to mission success.

The survivability goal is to remain undetected, or if detected to be difficult to hit. Once hit, the goal shifts to being able to withstand the hit(s) and still survive. The vulnerability of an aircraft is influenced by the aircraft's design and the choice of survivability features that reduce the amount and/or severity of damage when the aircraft is hit. Typical threat damage mechanisms include penetrators and fragments from missile and gun high explosive warheads, blast and the most recent threat from various high power radiation sources (e.g. electromagnetic pulse, particle beam and laser).

Aircraft designers do not generally choose a digital avionics system architecture because of its effect on the survivability of the aircraft, but rather for its performance advantages. Combat experience gained in the 1950s, 1960s and 1970s in Korea, Southeast Asia and the Middle East shows that aircraft were lost primarily due to damage to the fuel system, engines, flight controls, hydraulic systems and crew [Ref. 3: p 134]. The aircraft then in use did not incorporate extensive digital avionics systems. Modern tactical aircraft which incorporate extensive digital avionics systems were introduced in the mid-1970s and have seen only limited combat use. As a result, we have limited data on the causal factors leading to the loss of modern tactical aircraft and specifically to the contributions of digital avionics systems to aircraft combat survivability.

One characteristic of a modern digital avionics system is its high level of signal integration, as compared to older avionics systems. This integration is a key element in improving the efficiency and capability of the aircraft and is one of the reasons for its improved performance. However, the fact that the majority of the avionics devices are dependent upon information shared over the data buses is a disadvantage when the data bus information flow is interrupted or corrupted. For example, in the case of fly-by-wire flight control systems on unstable aircraft, where the control of the aircraft is dependent upon maintaining a continuous path between the flight control computer and the control surface servo actuators, combat damage that interrupts or corrupts this information flow could result in the loss of aircraft control. Thus, the choice of a digital avionics architecture can have an impact on the overall combat survivability of the aircraft.

C. SURVIVABILITY ASSESSMENT

Traditional methods of assessing the effects of component failure or damage to an aircraft fall within the discipline of system safety engineering. System safety engineering conducts hazard analyses (also called system safety analyses) of an aircraft in order to identify actual and potential hazards. Hazards are then assessed by considering the hazard severity and potential frequency of occurrence. Once identified and assessed, methods of resolving the hazards are proposed. System safety engineers use critical component analysis tools such as the Fault Tree Analysis (FTA) and the Failure Modes and Effects Analysis (FMEA).

A Fault Tree Analysis (FTA) is a top-down approach which begins with a given undesired event, such as loss of control, and then traces the possible causes of that event [Ref. 4: p. 17]. A Failure Modes and Effects Analysis (FMEA) is a bottom-up approach that identifies and records all possible failure modes of a component or subsystem and determines the effects of these failure modes. The effects are then linked to the ability of the component or subsystem to perform essential functions [Ref. 4: p. 11]. The FMEA does not specify the cause of the component failure. When failures caused by combat damage are investigated, the process is called a Damage Mode and Effects Analysis (DMEA) [Ref. 3: p. 142]. While it is not necessary to do both, combining the top-down approach of Fault Tree Analysis (FTA) with the bottom-up approach of the Failure Modes and Effects Analysis (FMEA) can give a representative picture of the impact of various component failures. After an FTA and/or FMEA has been conducted, a Vulnerability Assessment (VA) of the aircraft can be made.

A Vulnerability Assessment is the process of assigning numerical values for the various measures of vulnerability. Vulnerable area, defined as that area on the aircraft which if hit would cause a kill of the aircraft, is one such measure [Ref 3: p.153]. Numerical assessment can be done through the use of computer programs, such as the Computation of Vulnerable Area and Repair Time (COVART) program [Ref. 5]. COVART is a product of the Joint Technical Coordinating Group for Munitions Effectiveness, Aerial Target Vulnerability Working Group, and is used to determine the vulnerable area of aircraft damaged by the impact of single kinetic-energy penetrators.

D. THESIS ORGANIZATION

The contributions of modern digital avionics systems to the survivability of tactical aircraft are examined in this thesis. Each of the following systems within the general class of avionics is discussed:

- Flight control systems
- Engine control systems
- Flight avionics systems

- Tactical sensor systems
- Computer systems

Chapter II provides background information on digital avionics systems and architectures, summarizing their key features and characteristics. The focus of Chapters III and IV is on the contributions of the avionics systems and architectures to aircraft susceptibility and vulnerability, respectively. Chapter V discusses a proposed methodology by which the contributions of an avionics system to the vulnerable area of a tactical aircraft can be computed. Chapter VI contains design guidance and recommendations to reduce the vulnerability of digital avionics systems in order to increase a tactical aircraft's combat survivability.

II. DIGITAL AVIONICS SYSTEMS BACKGROUND

A. DIGITAL AVIONICS

The commonly applied definition of **avionics** includes all analog and digital electronic devices that are used in aircraft. Older analog systems that use variable resistance, capacitance and inductance and have an analog output signal are no longer the basis for new designs. Most modern aircraft use a digital avionics system that is made up of sensors, displays, data buses and microprocessors that are combined to perform various operations on binary electronic signals.

The binary signals are typically shown as **yes** equals one, or positive voltage, and **no** equals zero, or negative voltage, although the reverse is also possible. The output of the system operations is a string of ones and zeroes, encoded in accordance with a specific signal protocol that travels throughout the aircraft on digital data buses.

In a digital avionics architecture, the tasks are functionally allocated between the software, hardware and crew [Ref. 6: p. 8]. The level of integration is dependent upon the choice of avionics architecture, the size of the crew and the number of avionics systems to be integrated. The design choice of a digital avionics system is primarily important because of the additional capabilities, such as weapons, sensors or displays, that can be utilized by the aircraft and crew. Digital avionics systems can contribute [Ref. 6]:

- advanced sensors, processors and displays
- expert systems
- sensor fusion/weaponization

- improved command, control, communications and navigation

to the overall capabilities of the tactical aircraft.

B. DIGITAL AVIONICS ARCHITECTURES

Three main types of digital avionics architectures are available to the designer; federated, centralized (or integrated) and distributed [Ref. 6: p. 119]. Each type has specific characteristics, advantages and disadvantages, with the optimum choice dependent upon aircraft and mission requirements.

The majority of current generation aircraft (e.g. F-16, F/A-18) incorporate a federated architecture. Many earlier generation aircraft (e.g. F-14, A-10) are being retrofitted with a hybrid federated architecture. Future generation aircraft (e.g. F-22, JAST derivatives) will probably incorporate either a centralized architecture or a distributed architecture.

The federated architecture is shown in Figure 1. "A federated architecture is characterized by each major system, ..., sharing input and sensor data from a common set of hardware, and consequently sharing their computed results over data buses [Ref. 6: p. 119]." This design allows for relatively independent systems which combine in using a common data base. As a result, there is a degree of compartmentalization inherent in this architecture. A federated system in a military aircraft typically shares data over the MIL-STD-1553B data bus.

Some future generation aircraft will probably incorporate the centralized architecture shown in Figure 2. "A centralized architecture is characterized by signal conditioning and computations taking place in one or more

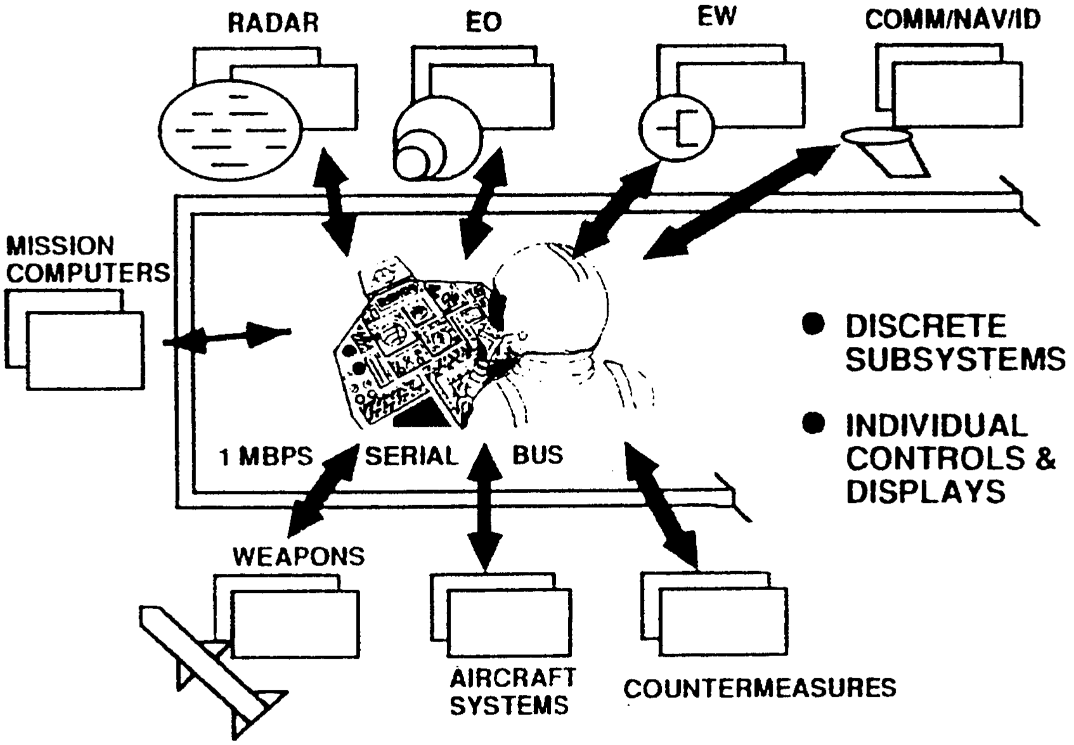

Figure 1. Federated Avionics Architecture, after Ref. [1]

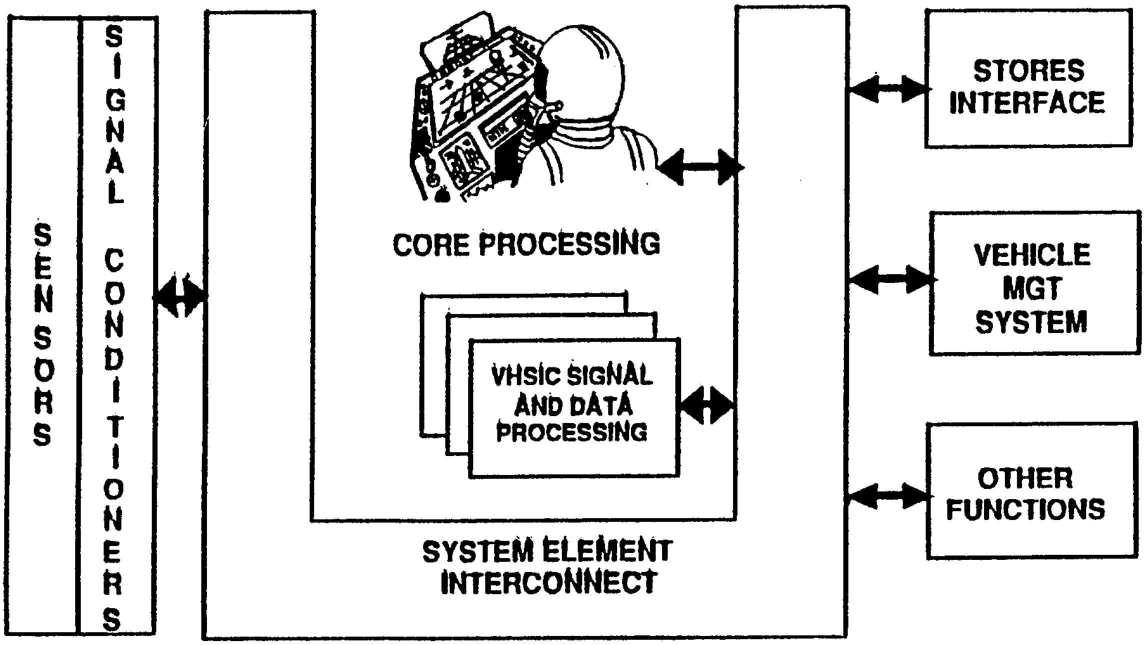

Figure 2. Centralized (Integrated) Architecture, from Ref [1]

computers...located in the avionics bay with sensor and command signals transmitted over data buses [Ref. 6: p.120]." This type may also be called an integrated architecture [Ref. 1: p. 6]. A centralized system in a military aircraft may use several different kinds of data buses, depending on the performance requirements.

The distributed architecture that is being evaluated for use in future tactical aircraft combines many of the features of both the federated and centralized architectures, as shown in Figure 3. "A distributed architecture has multiple processors throughout the aircraft that are assigned computing and control tasks in real time by executive software as a function of mission phase and/or system status [Ref. 6: p.120]." These distributed processors may perform significant amounts of signal processing at or near the sensors or actuators. A distributed system in a military aircraft is likely to use several high performance digital data buses, possibly based on civil computer networking standards.

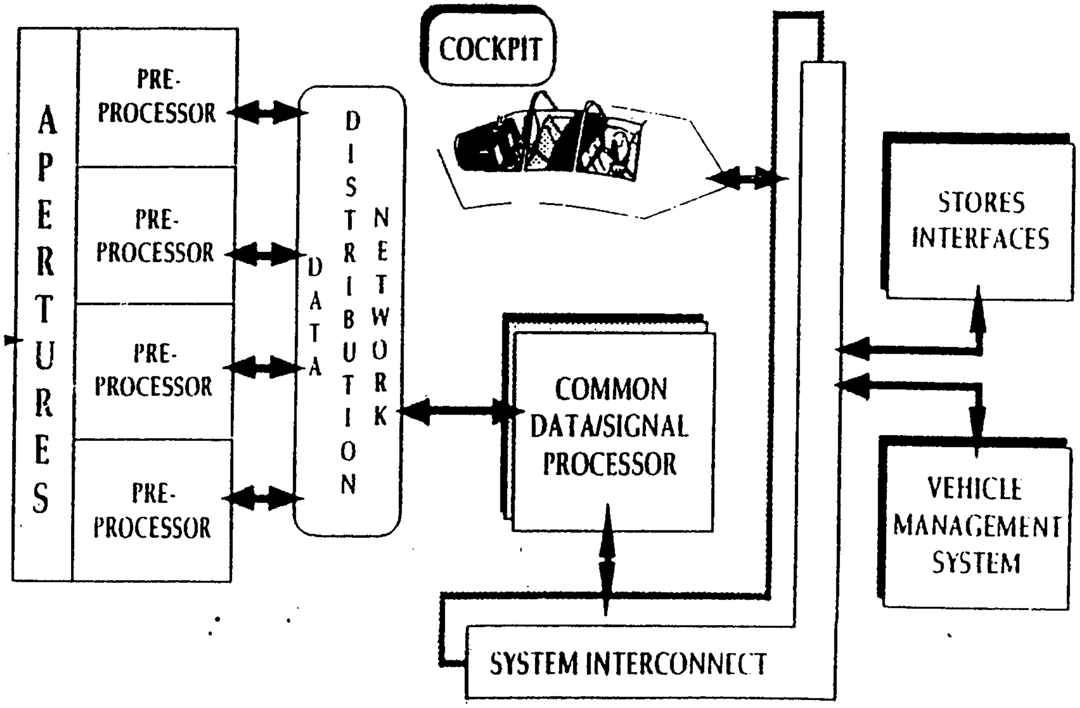

Figure 3. Distributed Architecture, from Ref.[1]

C. AIRCRAFT ELECTRICAL POWER

In all digital avionics system architectures, there is an assumption of reliable, uninterrupted electrical power. With analog avionics systems, it was relatively easy to design systems that were insensitive to interruptions in aircraft power and tolerant of voltage or frequency variations. The aircraft power system for modern digital avionics systems is not so easy to design. Most digital systems, especially microprocessors, are highly intolerant of interruptions in power and many are sensitive to variations in supply voltage and frequency. The requirements of MIL-STD-704: Aircraft Electrical Power Characteristics [Ref. 7] for military aircraft, or RTCA document DO-160: Environmental Conditions [Ref. 8] for commercial aircraft, detail the aircraft electrical power environment.

These two standards describe the over and under-voltage conditions, frequency variations, power interruptions and other conditions that the designer must accommodate. Of particular interest to the designer is the assumption that military aircraft electrical power systems may exhibit power interruptions of up to 50ms under transfer conditions [Ref. 6: p. 79], while power interrupts of up to 1s can be expected in civil aircraft [Ref 6: p. 81]. This is a significant design driver, especially for volatile microprocessor memory. The use of static random access memory (SRAM), which retains its contents only so long as power is applied, usually causes a designer to specify an alternate or back-up to the aircraft power supply. Some types of dynamic random access memory (DRAM), which use capacitance to retain memory contents and which depend on periodic refresh cycles, may also cause the designer to consider an alternate or back-up power supply. The criticality of the avionics function determines whether a given device requires uninterrupted power or not.

The aircraft electrical loads are characterized as either critical, essential or utility [Ref. 6: p. 88]. Critical loads include flight control systems, cockpit flight instruments and cockpit displays. The nature of these systems demands that multiple, redundant power buses be provided and that provisions for uninterruptable power be made available. Avionics systems of lesser criticality are typically referred to as essential loads, examples of which are the tactical sensors. Systems that are not essential to safe flight, such as galley equipment or entertainment systems, are usually referred to as utility loads. Redundant power generation and storage systems for the critical and essential loads are typically specified in order to obtain the required reliability of the avionics system and to provide backups in case of malfunction or damage.

D. AVIONICS DATA BUSES

1. Military Aircraft

The digital avionics data buses may be thought of as the nervous system of the aircraft, with multiplexed signals being shared between systems connected by the data bus. Current military aircraft typically incorporate the MIL-STD-1553B data bus, with some aircraft incorporating the fiber-optic cable version of the 1553B protocol, the MIL-STD-1773 data bus. Future tactical aircraft are likely to incorporate the High Speed Data Bus (HSDB), probably in combination with the 1553B and 1773 data buses. It is also likely that avionics equipment incorporating either of the commercial data bus standards, ARINC 429 or ARINC 629, will be used on military aircraft.

The MIL-STD-1553B data bus is characterized by the use of time-division multiplexing and a bus controller. The bus controller functions as a "traffic cop" to prevent two or more devices from transmitting simultaneously. If the bus controller fails, the data bus is rendered inoperative. The data bus protocol and the message formats are called out in the specification document [Ref. 9].

The 1553B operates at the relatively slow data transfer rate of 1 MBit/s. In order to increase reliability and reduce electromagnetic interference, the 1553B data bus uses a twisted, shielded pair of wire cables which is routed through the aircraft. Typical cable design is shown in Figure 4. Depending on the criticality of the function, some aircraft use as many as four 1553B data buses in parallel.

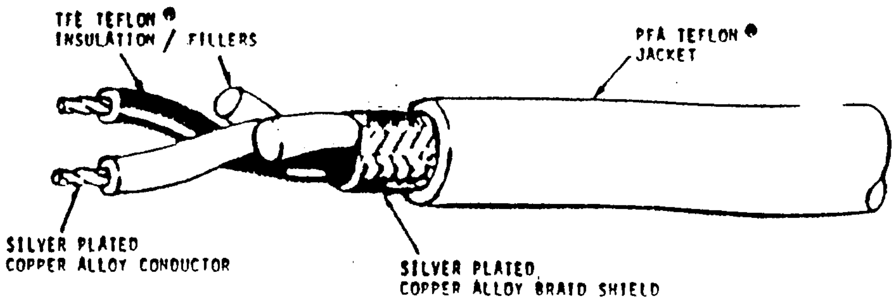

Figure 4, MIL-STD-1553B Cable, after Ref [9]

The DOD-STD-1773 digital data bus [Ref. 10] is a fiber-optic cable implementation of the same data bus protocol used in the 1553B. The intent of the change to fiber-optic cables was to reduce the possibility of electromagnetic interference and to reduce weight. The current implementation is restricted to 1 MBit/s, although the possibility exists to increase the data transfer rate of the 1773 data bus to 8 MBit/s in the enhanced mode. The 1773 data bus incorporates most of the features of the 1553B, including a bus controller, with the twisted, shielded cable replaced by a fiber-optic cable, such as Figure 5.

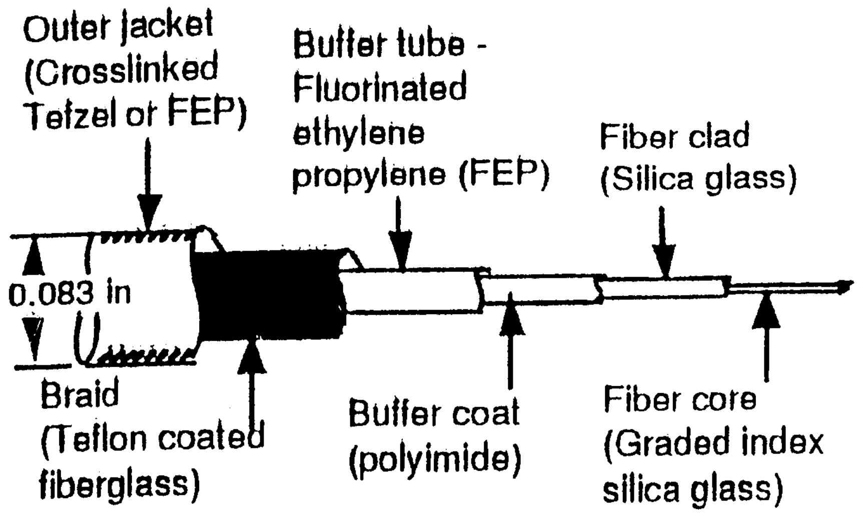
Outer jacket (Crosslinked Tefzel or FEP)
Buffer tube - Fluorinated ethylene propylene (FEP)
Fiber clad (Silica glass)
0.083 in
Braid (Teflon coated fiberglass)
Buffer coat (polyimide)
Fiber core (Graded index silica glass)

Figure 5, DOD-STD-1773 Fiber-Optic Cable, after Ref [10]

The latest military standard digital data bus is the High Speed Data Bus (HSDB), which was developed by the Air Force to provide a much increased rate of data transmission [Ref. 11]. The HSDB can transmit data at up to 50 MBit/s and can use several different bus topologies in either the conventional twisted, shielded pair or fiber-optic cable implementations. A key design feature of the HSDB is a "token passing" control architecture, which removes the requirement for a bus controller. This is a key design advantage of the HSDB over the earlier MIL-STD 1553B or DOD-STD-1773 data bus designs because a single point of failure (kill) has been avoided.

2. Civil Aircraft

The civil standards for digital data buses in transport aircraft are the ARINC 429 [Ref. 12] and ARINC 629 [Ref 13]. The ARINC 429 digital data bus is a simplex bus in which there is only one transmitter but multiple receivers. This design choice avoids the use of a bus controller, although it does require the use of multiple data buses. There is a requirement for a dedicated ARINC 429 data bus for each pair of avionics devices that must transfer information to one another. The ARINC 429 uses a twisted, shielded pair wire cable very similar to that used by the MIL-STD-1553B. The rate of data transmission is slower than the 1553B, at either 12 to 14.5 KBit/s (low speed) or 100 KBit/s (high speed). Because the ARINC 429 is a simplex bus with a single transmitter, there are multiple ARINC 429 data buses. This increases reliability and eases certification at the cost of additional weight and complexity.

The latest civil digital data bus standard is the ARINC 629. This is a multi-transmitter data bus that also does not require a data bus controller. In the ARINC 629 design, each avionics device is granted autonomous access to the bus based on a complex timing scheme. The rate of data transmission, at 2 MBit/s, is faster than the 1553B and the ARINC 629 can use any one of three cable designs: wire, with either inductive or voltage coupling and optical fiber. The use of inductive coupling avoids the weight penalty associated with cable shielding, since the data bus signals are current-coupled instead of voltage-coupled. This data bus has been chosen for use in the Boeing 777.

E. MICROPROCESSORS

Recent advances in microelectronic technology have made it possible to use computers as an integral part of avionics systems. Miniaturized digital computers are typically referred to as microprocessors, or even as "chips", because they are usually contained on a single integrated circuit

(I.C.) chip. They are used for many different functions (e.g. numeric calculations, control, graphics displays and signal processing). Because of their small size and robust capability, these devices are found in nearly all avionics systems.

Microprocessors, as a group, are generally understood to include both general purpose computers and digital signal processors. Within general purpose computers, microprocessors are divided into Complex Instruction Set Computer (CISC) and Reduced Instruction Set Computer (RISC) types. [Ref. 1: p. 70]

The most common type of microprocessor is the CISC chip, characterized by the various MIL-STD-1750A 16-bit computer chips and the Intel 80X86 series chips that are popular in personal computers. These are general purpose microprocessors which incorporate the hardware and software needed to carry out many different complex operations. Their internal operations may take one, two or even several cycles to complete. CISC computers are very flexible and powerful and serve as the "brains" of many avionics systems.

An emerging microprocessor type is the RISC chip, characterized by the Sun SPARC and the Motorola Power PC chips. These are general purpose microprocessors whose design has been optimized to support completion of internal tasks within a single cycle. RISC computers are more efficient than the CISC design, although they require software that is optimized for the smaller number of instructions. RISC chips have found significant use as the "engines" for work stations and are finding uses aboard aircraft avionics systems.

The third type of microprocessor is the Digital Signal Processing (DSP) chip. The DSP chip is usually dedicated to signal processing applications where extremely efficient input/output capability is important due to the sheer volume of data to be processed. DSP chips are commonly found in avionics sensor systems (e.g. radars, acoustic processors).

F. SENSORS

There are many avionics devices that detect and respond to electromagnetic, e.g. infrared or visual wavelength, signals. These include both active devices, which can transmit signals, and passive devices, which only receive signals. Examples of active devices include radar sets and radio communication systems. Examples of passive devices include infrared detection systems and radio navigation receivers.

G. AVIONICS DISPLAYS

The cockpits of today's modern tactical aircraft and civil air transport aircraft are now host to numerous programmable displays and crew interface devices. The familiar analog, electro-mechanical gauges that were the standard for the 1950s through early 1970s aircraft cockpits have largely been replaced by systems incorporating either cathode ray tube (CRT) or liquid crystal display (LCD) technology. These video display devices provide the same sort of information to the pilot; heading, altitude, direction, speed, navigation cues, etc. The format of the display is in many cases similar or even identical to the electro-mechanical device that the CRT or LCD replaces. However, the video displays are not limited to emulating the older analog devices. They can be programmed to combine the information that formerly required two or more instruments to display into a single "picture" for the pilot. For the crew interface devices (e.g. multifunction display control panels) the new touchpads, keys and digital readouts have replaced the familiar knobs and dials of earlier aircraft cockpits.

These new digital displays and crew interface devices are based on the use of microprocessors for control of the video display. The cockpit instruments, especially the flight instruments, are generally considered to be critical systems. As a result, the certification of software as well as hardware has emerged as a significant design driver in digital avionics systems.

The flight critical CRT or LCD displays must: be assured of reliable, uninterrupted power; have software that is demonstrated to be reliable in use; and have hardware that meets or exceeds the reliability standards for the application. Thus, the possibility of damage to the display itself, the interconnecting wiring or data bus, the power supply and the source of information to be displayed must be considered when examining safety and survivability. The possibility of damage to the software, or of a hidden "bug" in the software, is also a concern. Damage to any one of these elements could cause failure of the cockpit display systems and contribute to loss of control of the aircraft.

III. SUSCEPTIBILITY EFFECTS

A. SUSCEPTIBILITY

Aircraft combat survivability is made up of two elements: susceptibility, the inability of the aircraft to avoid being damaged by the various elements of the man-made hostile environment; and vulnerability, the inability of the aircraft to withstand the damage caused by the man-made hostile environment [Ref. 3]. Since the susceptibility of an aircraft is influenced by the aircraft's design, tactics, equipment and weapons, the contributions of a digital avionics system should be measured by both direct and indirect contributions to susceptibility reduction. This chapter will explore those contributions of the digital data buses used in digital avionics systems to the susceptibility of an aircraft.

The choice of a digital avionics system will have an effect on the six major concepts for reducing susceptibility [Ref. 3]:

- Threat warning.
- Noise jamming and deceiving.
- Signature reduction.
- Expendables.
- Threat suppression.
- Tactics.

B. THREAT WARNING

The first of these susceptibility reduction concepts, threat warning, refers to aircraft systems that provide information on the location, type and status of the threat elements in the vicinity of the aircraft. Examples of threat warning systems include: radar warning receivers, laser warning receivers and missile approach warning systems.

These systems can be installed in an aircraft in a "stand alone" mode, with discrete wiring, controls and display(s) for each individual system. If a digital data bus design is used instead, the connectivity options that are available make it possible to replace many of the discrete portions of the system. For example, the data bus can be used to interconnect the antenna(s), processor, controls and displays of a threat warning system. A higher level of integration is also possible, where the control and display functions are shared with other systems. If the display processor is sufficiently capable, sensor fusion techniques, such as correlating radar returns with threat warning data, are possible. Another indirect benefit of the use of a data bus can be to allow for queuing of an expendables launcher, based on the threat warning system. Therefore, the contributions of a digital data bus to the susceptibility reduction factor of threat warning are due to the connectivity, shared control and shared displays, along with options for sensor fusion and queuing of expendables.

C. NOISE JAMMING AND DECEIVING

The second susceptibility reduction concept is noise jamming and deceiving, also called "jamming", "spoofing" or "defensive electronic countermeasures (DECM)". There are many different techniques available, each of which exploits some weakness in the threat system.

As with threat warning, these active noise jamming and deceiving systems can be installed in an aircraft in a "stand alone" mode, with discrete wiring, controls and display(s) for each individual system. If a digital data bus design is used instead, the connectivity options that are available make it possible to replace many of the discrete portions of the system. Queuing of an expendables launcher in concert with the noise jamming and deceiving system is also possible. Therefore, the contributions of a digital data bus to the susceptibility reduction factor of noise jamming and deceiving are due to the connectivity, shared control and shared displays, along with the option for queuing of expendables.

D. SIGNATURE REDUCTION

The third susceptibility reduction concept is signature reduction, sometimes referred to as "stealth". Signature reduction typically encompasses the radar, infrared, noise and visual signatures. The digital data bus itself gives off virtually no electromagnetic or noise signature that is detectable outside the aircraft since it operates at very low voltages within either a shielded cable or a fiber optic cable.

However, a major consideration of radar signature reduction is to reduce the number and size of radar reflectors, of which antennas are a prime example. The use of a digital data bus, with its options for connectivity, can make possible the sharing of sensor apertures, thus reducing the number and/or size of the antennas and hence the radar signature.

E. EXPENDABLES

The fourth susceptibility reduction concept is the use of expendables, usually understood to include chaff, flares, active jammers and aerosols. Expendables are usually designed to counter radar, infrared and visually directed weapons.

As with threat warning, these expendables systems can be installed in an aircraft in a "stand alone" mode, with discrete wiring, controls and display(s) for each individual system. If a digital data bus design is used instead, the connectivity options that are available make it possible to replace many of the discrete portions of the system. Queuing of an expendables launcher in concert with the noise jamming and deceiving system or in concert with the threat warning system is also possible.

F. THREAT SUPPRESSION

The fifth susceptibility reduction concept is threat suppression, generally understood as a means of either keeping the bad guys from shooting at you or destroying their ability to shoot back. Lethal threat suppression systems may be carried either on specialized aircraft (e.g. "Wild Weasel") or on one's own aircraft and include various means of delivering ordnance on target, such as anti-radiation missiles.

An emerging use of digital data bus systems is to provide for onboard programming of threat suppression weapons. Either onboard or off-board sensors can be used to provide queuing to the threat suppression system, which can then program the weapon to respond to the specific type and location of the threat. This capability extends the tactical utility of the threat suppression system.

G. TACTICS

The sixth and last susceptibility reduction concept is tactics. The integration of multiple sensors, using sensor fusion techniques, and the options for automatic queuing of expendables and threat suppression systems are contributing to the rapid evolution of new tactics. As an example, a recent article [Ref. 14] reported the use of off-board targeting (from an EA-6B) to provide threat information in support of the launching of a threat suppression weapon system (an F-16 carrying a HARM missile). The aircraft involved made use of digital data buses and a digital data link to transfer information among the various systems.

IV. VULNERABILITY EFFECTS

A. VULNERABILITY

Vulnerability is the inability of the aircraft to withstand the damage caused by the man-made hostile environment [Ref. 3]. Each of the components in the aircraft has a degree of vulnerability which contributes to the overall aircraft vulnerability. Components whose loss of function or kill mode would lead to the kill of the aircraft are referred to as critical components [Ref. 3: p. 137]. A kill mode refers to the reaction of the component or system when hit, such as a fire or explosion. Identification of these critical components and their kill modes is a key part of a vulnerability assessment.

B. KILL CATEGORIES

The discipline of aircraft combat survivability provides definitions for the aircraft kill categories, further divided into two sub-categories:

- Attrition, where the aircraft is lost to inventory. There are four levels of attrition:

KK=	catastrophic (immediate loss of control)
K=	loss of control within 30 seconds after a hit
A=	loss of control within 5 minutes after a hit
B=	loss of control within 30 minutes after a hit

- Mission Abort, where the aircraft returns to base, but does not complete the mission due to combat damage.

Because of the nature of electronics devices, combat damage is likely to result in either the immediate loss of function or the component will survive. From an avionics perspective, the most likely causes of an attrition kill would be by damage to the flight control system in a "fly-by-wire" aircraft or to the primary flight display system in a "glass cockpit" aircraft. Most other damage to avionics is more likely to result in a mission abort kill [Ref. 15: P. 9].

C. DAMAGE MECHANISMS AND DAMAGE PROCESSES

A damage mechanism is the output of the warhead that causes damage to the target, sometimes referred to as a kill mechanism [Ref. 3: P. 84]. For an avionics system, the damage mechanisms of interest include:

- penetrators/fragments (from warheads or projectiles)
- blast, incendiary
- electro-magnetic pulse (EMP)

These damage mechanisms cause resultant damage processes, such as penetration and combustion, when they interact with the aircraft. Terminal effects refer to the ultimate response or effect of the damage mechanism on the aircraft components. These terminal effects can lead to a specific kill mode, which is defined as a damage-caused failure of a component [Ref. 3: p. 142]. Kill modes for avionics components may include:

- severing (a physical break in a wire)
- grounding (signal diverted to ground)
- corrupting (signal degradation due to damaged EM shield or EMP)
- loss of integrity (crushed, casing penetrated, etc.)
- overheating (resulting from fire or explosion)

The effect of these damage mechanisms on the survival of the aircraft varies depending on the criticality of the component(s) affected.

D. VULNERABILITY ASSESSMENT

A Vulnerability Assessment is the process of assigning numerical values for the various measures of vulnerability, i.e. vulnerable area [Ref 3: p.153]. The general requirements for conducting a vulnerability assessment are [Ref. 3]:

- Select a kill category and level
- Assemble the aircraft technical and functional description
- Determine the critical components and their kill modes for the selected kill category and level
- Select the threat
- Determine the critical component kill criteria
- Compute the vulnerability measure for the selected threat and kill category and level

The first task in a vulnerability assessment is to identify the critical components and their kill modes. Once the critical components and their kill modes have been identified, a vulnerability assessment can be conducted to quantify the measures of component and aircraft vulnerability, expressed in terms of vulnerable area to a specific threat.

The vulnerability assessment is typically presented in a graphical form, known as either a "kill tree" or "fault tree". An example is shown as Figure 6. This graphic presentation method is used by survivability engineers, with any break in a vertical line joining the critical components representing an assumed result of an aircraft kill. This is a variation of survivability logic diagrams, which are related to reliability (logic) diagrams, where possible failure modes and outcomes are displayed in a logic diagram. In reliability engineering, damage due to hostile action is usually excluded from the discussion.

Vulnerability is expressed in relation to a specific man-made threat, such as 23mm High Explosive Incendiary (HEI) shells. For most aircraft, there will be areas where the aircraft can withstand a hit by a 23mm HEI, while in more critical areas, such a hit could damage a critical component, leading to loss of the aircraft. The vulnerable area (Av) is a theoretical area of the aircraft which is presented to the threat from a particular direction that, if hit in this area, would result in an aircraft kill [Ref.3: p.154]. The ratio of the aircraft's vulnerable area to its presented area represents the probability that the aircraft is killed given a random hit on the aircraft (Pk/h) [Ref. 3: p.154]. Once the vulnerabilities of the aircraft are understood, design features can be used to reduce vulnerability.

These vulnerability reduction features can have a cost and weight penalty. One of the major uses of the vulnerability assessment is to predict the probable reduction in aircraft losses in the event that the aircraft is equipped with specific survivability enhancement features. The cost of these features can then be related to the probable cost savings expressed in aircraft and aircrew not killed. This information can then be used to support a decision on whether to include a certain vulnerability reduction feature, or not, based on the anticipated benefits versus the probable costs.

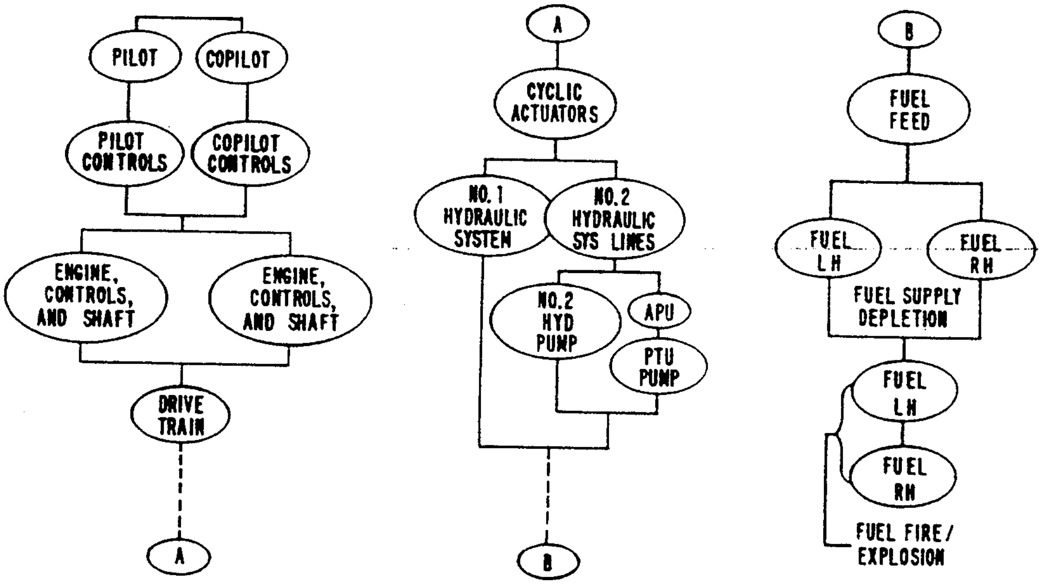

Figure 6, Example Kill Tree For a Two Engine, Two Pilot Helicopter, From Ref. 3

E. CRITICAL COMPONENTS

The general definition of a critical component is one whose loss leads to a loss of function or whose kill mode leads to an aircraft kill. Also considered are critical components whose loss of function or kill mode would lead to the kill of another critical component that provides an essential function. [Ref. 3]. Critical components may be either redundant or non-redundant.

For the purposes of this thesis, the focus will be on the critical components of the avionics system, especially the data buses. In general, a data bus consists of remote terminals, couplers and a cable (wire or fiber optic). The data buses provide for the connectivity between the various avionics devices. These avionics devices exist as remote terminals on the data buses.

A remote terminal can be a critical component, depending on the function that the individual remote terminal performs. The remote terminal that functions as the bus controller is a critical component in any data bus that uses a bus controller protocol (such as MIL-STD-1553B) if the loss of this data bus will lead to a kill of the aircraft. The loss of the bus controller or its functions will result in the loss of all data bus functions, unless a back-up bus controller is available. This is because of the command/response design protocol which employs a bus controller to de-conflict the various remote terminals, preventing simultaneous transmissions over the data bus.

Data bus couplers and associated stubs leading to remote terminals are of different design for each of the three transmission modes: voltage-coupled, current-coupled and fiber-optic. The failure of a coupler located between the data bus cable and a remote terminal that is a critical component could result in the loss of an essential function performed by that component. The data bus couplers in a voltage-coupled data bus are designed to electrically isolate individual remote terminals from the data bus and are unlikely to directly cause a data bus failure (Figure 7). The data bus couplers used in a current coupled data bus are extremely unlikely to directly cause a data bus failure because they do not require any break in the data bus cable (Figure 8). The data bus couplers used in a fiber-optic data bus could cause a data bus failure if badly damaged. Since they are permanently fused to the cable and have no moving parts, damage to the coupler would be likely to simultaneously damage the cable by disrupting the light path. In all three cases, couplers are critical components if the remote terminal that they serve is considered to be a critical component.

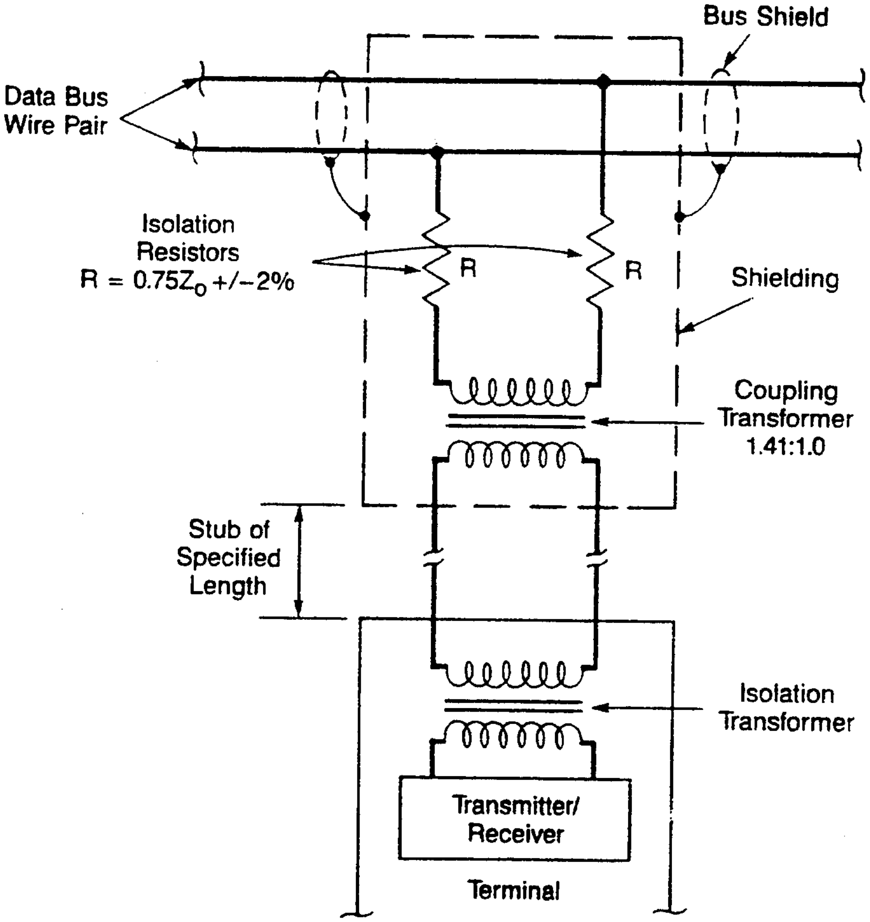

Figure 7, Data Bus Coupler, Voltage-Coupled (From Ref. 6)

The cable (wire or fiber-optic) that connects the various remote terminals is another critical component, if the loss of the data bus will lead to a kill of the aircraft. Severing of the wire or fiber-optic cable due to impact by a penetrator or by secondary means (e.g. fire, explosion) will generally result in loss of data bus function. Similarly, loss of cable shield integrity will be likely to disable the wire data bus if the signals are diverted to ground or are corrupted by electro-magnetic interference. A fiber-optic data bus can continue to function with a damaged shield as long as the light-transmitting fiber is intact.

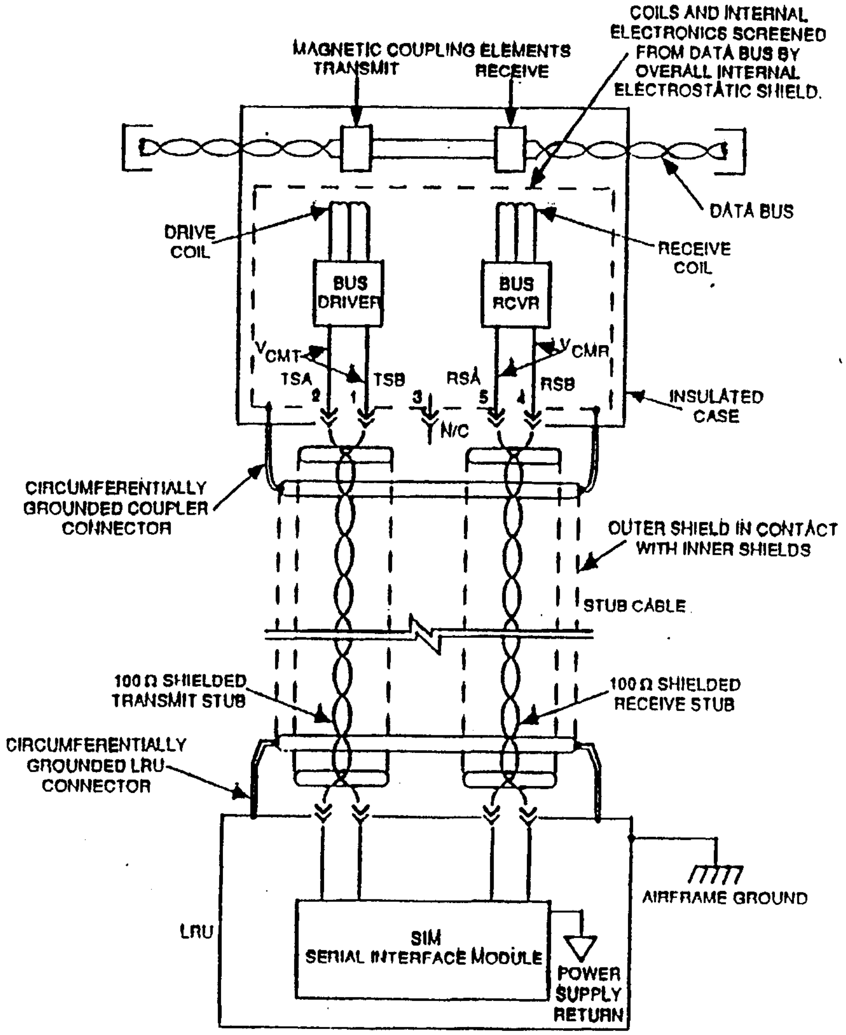
COILS AND INTERNAL ELECTRONICS SCREENED FROM DATA BUS BY OVERALL INTERNAL ELECTROSTATIC SHIELD.
MAGNETIC COUPLING ELEMENTS
TRANSMIT
RECEIVE
DATA BUS
DRIVE COIL
RECEIVE COIL
BUS DRIVER
BUS RCVR
V_{CMT}
V_{CMR}
TSA
TSB
RSA
RSB
2
1
3
5
4
N/C
INSULATED CASE
CIRCUMFERENTIALLY GROUNDED COUPLER CONNECTOR
OUTER SHIELD IN CONTACT WITH INNER SHIELDS
STUB CABLE
100 Ω SHIELDED TRANSMIT STUB
100 Ω SHIELDED RECEIVE STUB
CIRCUMFERENTIALLY GROUNDED LRU CONNECTOR
AIRFRAME GROUND
LRU
SIM SERIAL INTERFACE MODULE
POWER SUPPLY RETURN

Figure 8, Data Bus Coupler, Current-Coupled (From Ref. 13)

F. LOSS OF FLIGHT CONTROL (ATTRITION) KILL

An aircraft with a "fly-by-wire" or "fly-by-light" flight control system depends upon data buses to provide a reliable data path for the flight control signals. To ensure adequate reliability, three or four data buses operating in parallel are typically used. These data buses provide for communications between the flight control computer, inertial and air data sensors, flight control servos and other components of the flight control system.

The critical components of a "fly-by-wire" or "fly-by-light" flight control system include:

- flight control computers
- flight controls
- aircraft motion data sensors (INS, GPS, air data)
- data buses
- flight control servos
- flight control power systems (hydraulic or electric)
- flight control surfaces

From the perspective of the avionics system, these flight control systems can be disabled by the following kill modes:

- disruption of the control signal path
- loss of aircraft motion data (for unstable aircraft)
- fire/explosion/overheating

An aircraft kill could result from damage to the control signal paths from the pilots' flight controls to the flight control computer(s); damage to the data buses from the flight control computer such that the signals cannot reach their intended destination; and damage to aircraft motion data sensors or their connection to the flight control computer(s). If the aircraft is an unstable aircraft, such damage will be likely to result in an attrition kill. In a stable aircraft, such damage may result in a mission abort kill, assuming that there is a functional backup control system which provides the aircraft with a "get home" capability.

Figure 9 shows a sample "kill tree' that presents the critical components of a "fly-by-wire" flight control system in a graphical form [after Ref. 15]. The kill tree for the "fly-by-wire" flight control system shows the reduced vulnerability of the system that results from the use of multiple, redundant data buses for transmitting the flight control signals. However, there are possible single point failures for the flight control system at each of the flight control servo locations and at the flight control computer (which typically serves as the bus controller). This is because all of the data buses are in close proximity at these locations, since it is typical for all of the data buses to be used for pathways from the flight control computer to each of the flight control servos. A hit which disables the flight control computer(s), or a hit in the vicinity of the servos could conceivably disable all of the data buses simultaneously since cables and couplers are not hardened.

A hit that causes the failure of any of the critical components of an individual data bus (bus controller, cable and couplers to other critical components) could lead to failure of that individual data bus. Since only one of the other data buses has to survive in order to maintain system functionality, a minimum of one failure of a critical component in each of the data buses would be necessary to block the transmission of the flight control signals from the flight control computer to the servos.

Figure 10 shows a sample "kill tree' that presents the critical components of a "fly-by-wire" flight control system data bus in a graphical form [after Ref. 15].

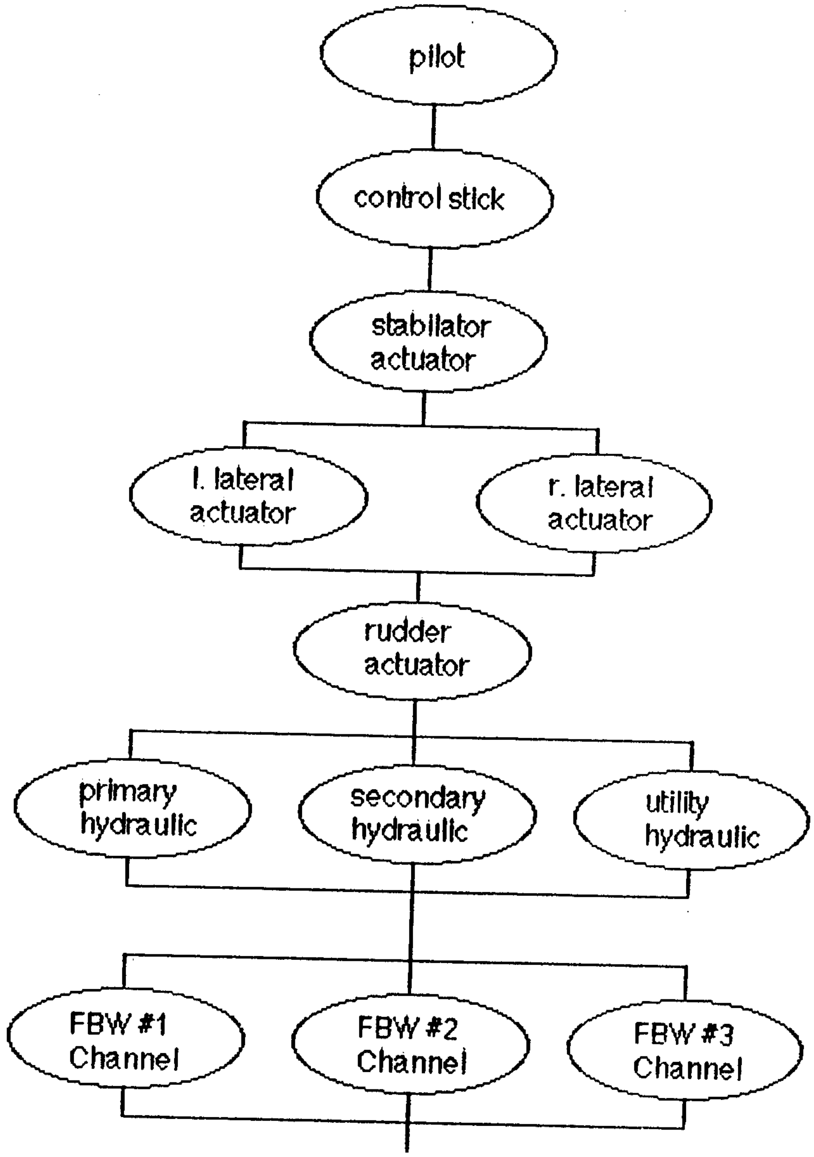

Figure 9, Flight Control (Attrition) Kill Tree

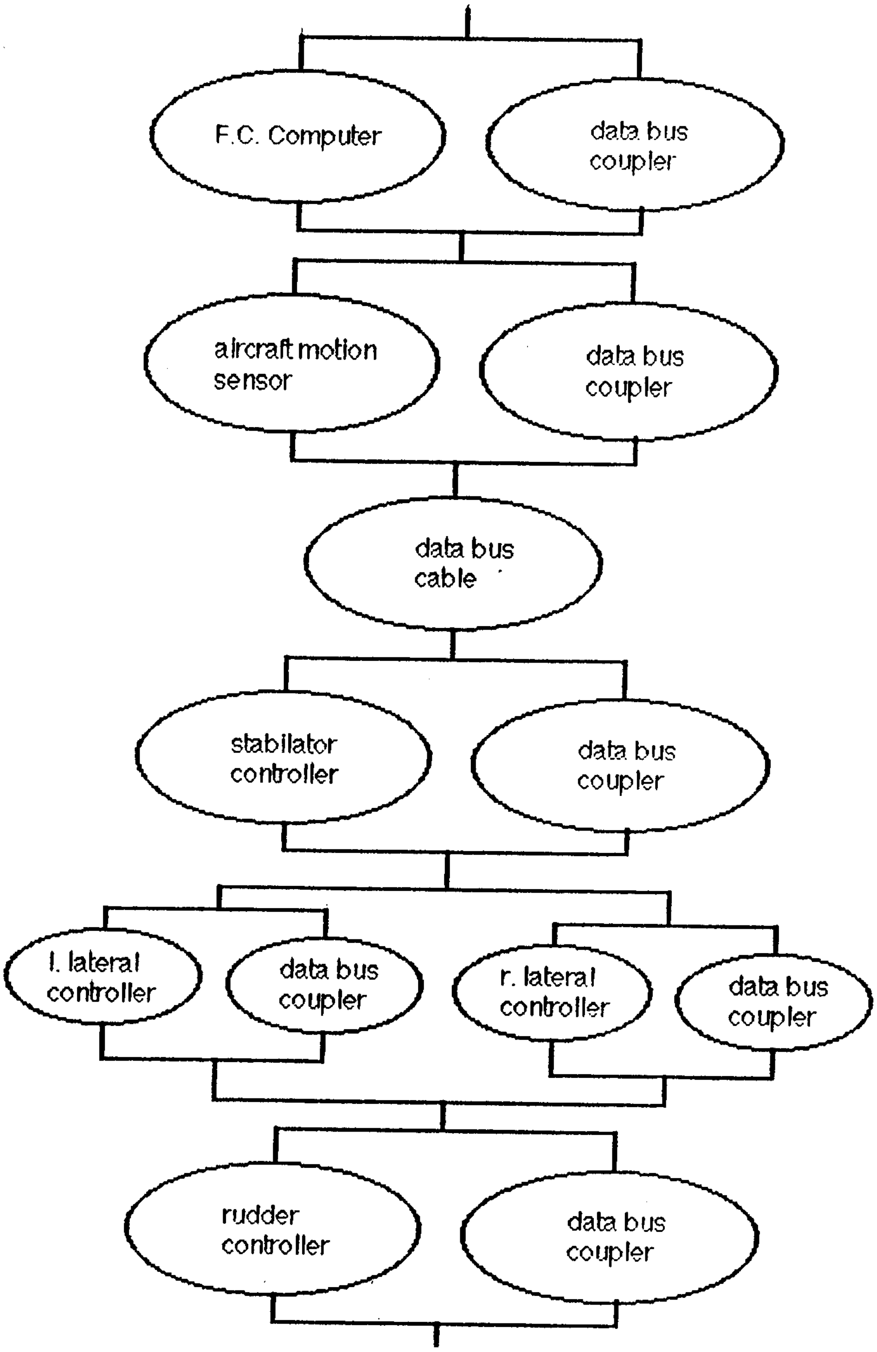

Figure 10, Flight Control Data Bus (Attrition) Kill Tree

G. LOSS OF ENGINE CONTROL SYSTEMS (MISSION ABORT) KILL

In general, combat damage to the engine electronic control systems will be unlikely to directly result in attrition, with a mission abort being a much more likely outcome. This is because of the stand-by or manual engine controls that are typically provided to give the pilot a "get home" capability. Loss of communications between the engine control systems and the air data reference systems due to damage to the data bus is one possible scenario that could lead to a mission abort. The critical components of an engine control system can include:

- data buses
- displays (e.g. CRTs or AMLCDs)
- display drivers
- flight reference systems (e.g. air data)
- throttles
- engine control computer(s)

From the perspective of the avionics system, these can be disabled by the following kill modes:

- penetrator/fragment damage leading to severing or grounding
- fire/explosion/overheating

The loss of an element or various elements of the engine control system may be considered sufficient to warrant a mission abort, depending on the nature of the mission.

The "kill tree" for the engine control system shows the reliance of the system on the data bus or data buses to share information and to manage the system. See Figure 11 for a sample "kill tree' that presents these critical components in a graphical form.

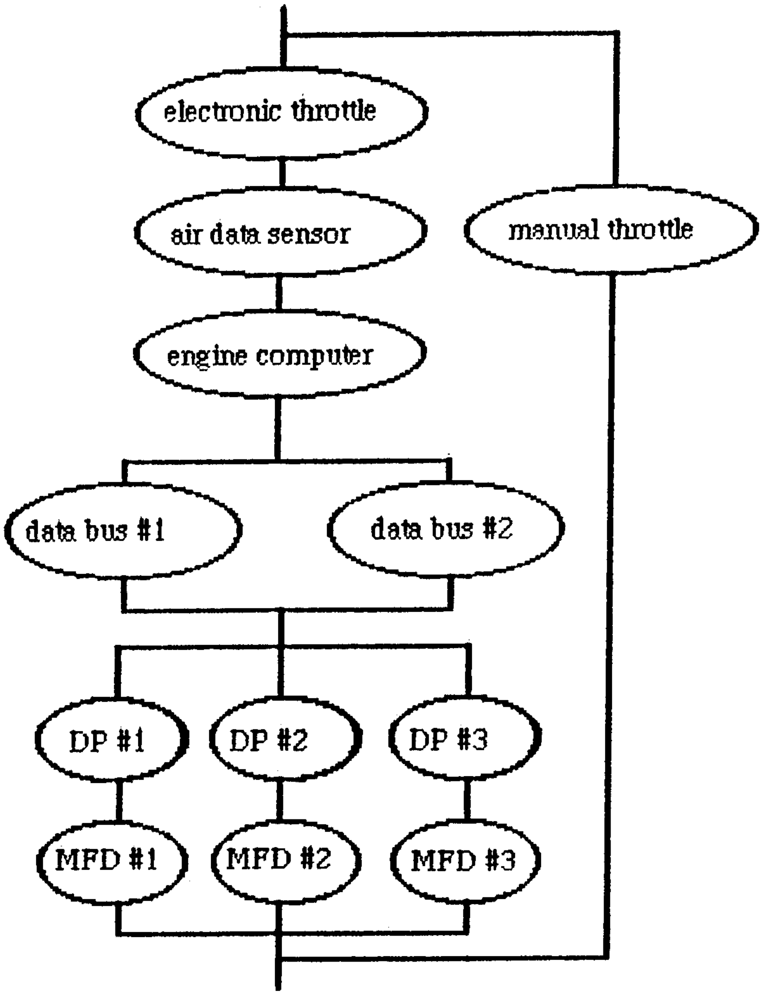

Figure 11, Engine Control System (Mission Abort) Kill Tree

H. LOSS OF FLIGHT AVIONICS (MISSION ABORT) KILL

In general, combat damage to the flight avionics is unlikely to directly result in attrition, with mission abort being a much more likely outcome. This is because of the stand-by or secondary flight instrumentation that is typically provided (e.g. "peanut" gyro), even in a "glass cockpit" aircraft, to give the pilot a "get home" capability. Loss of communications between the "glass cockpit" displays and the flight reference systems due to damage to the data bus is one possible scenario that could lead to a mission abort. The critical components of a flight avionics system can include:

- data buses
- displays (e.g. CRTs or AMLCDs)
- display drivers
- flight reference systems (e.g. gyros, motion sensors)
- central computer(s)

From the perspective of the avionics system, these can be disabled by the following kill modes:

- penetrator/fragment damage leading to severing or grounding
- fire/explosion/overheating

The loss of an element or various elements of the flight display system may be considered sufficient to warrant a mission abort, depending on the nature of the mission and environmental conditions.

The "kill tree" for the flight avionics system shows the reliance of the system on the data bus or data buses to share information and to manage the system. See Figure 12 for a sample "kill tree' that presents these critical components in a graphical form.

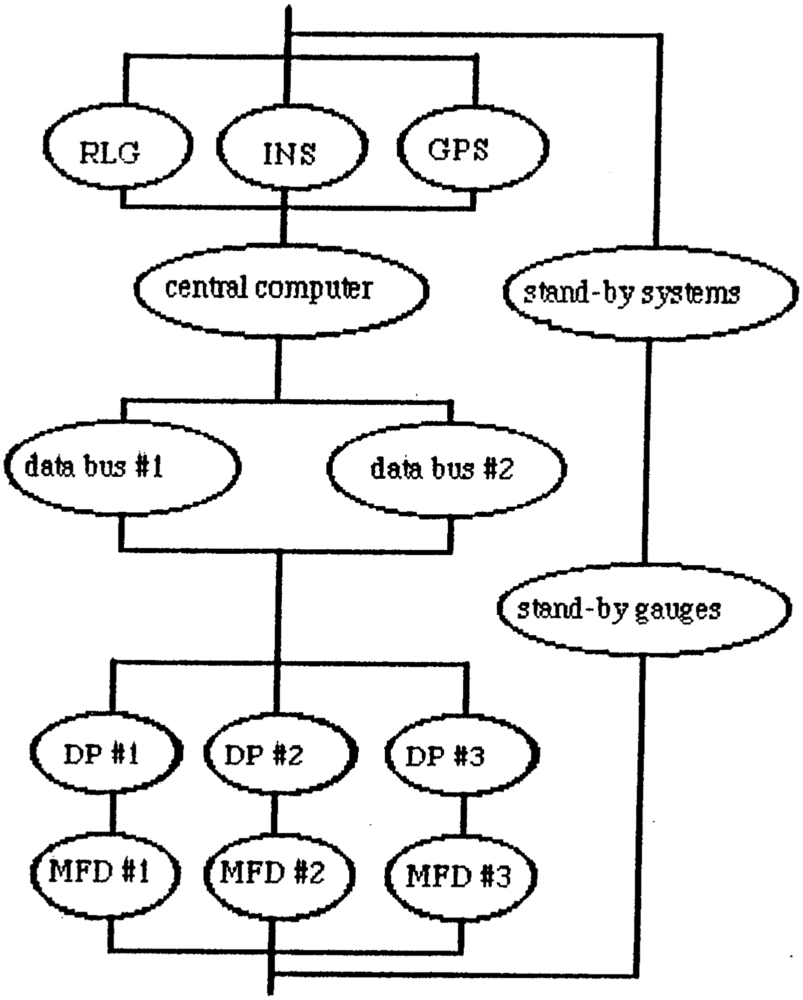

Figure 12, Flight Avionics (Mission Abort) Kill Tree

I. LOSS OF TACTICAL SENSOR SYSTEMS (MISSION ABORT) KILL

In general, combat damage to the tactical sensor systems is unlikely to directly result in attrition, with mission abort being a much more likely outcome. Loss of communications between sensors or between sensors and displays due to damage to the data bus is one possible scenario that could lead to a mission abort.

The critical components of a tactical sensor system can include:

- data buses
- displays
- threat warning & countermeasures systems
- central computer(s)
- sensors (radar, electro-optical, etc.)
- electronic warfare systems

From the perspective of the avionics system, these tactical sensor systems can be disabled by the following kill modes:

- penetrator/fragment damage leading to severing or grounding
- fire/explosion/overheating

The loss of an element or various elements of the tactical sensor system could be considered sufficient to warrant a mission abort, depending on the nature of the mission and magnitude of the expected threat.

The "kill tree" for the tactical sensor system shows the reliance of the system on the data bus or data buses to share information and to manage the system. Figure 13 shows a sample "kill tree' that presents these critical components in a graphical form. Whenever an avionics architecture that incorporates the tactical sensor systems via a data bus is used, there is a clear requirement for one or more backup data buses in order to ensure system integrity in the event of damage. Failure of any individual system (e.g. threat warning, countermeasures, radar, etc.) is unlikely to lead to a mission abort in all cases. However, failure of the entire data bus system or display system would most likely result in a mission abort. A crew may be able to continue the mission with a single sensor system disabled, but would be unlikely to continue the mission with a complete failure of all tactical sensor systems.

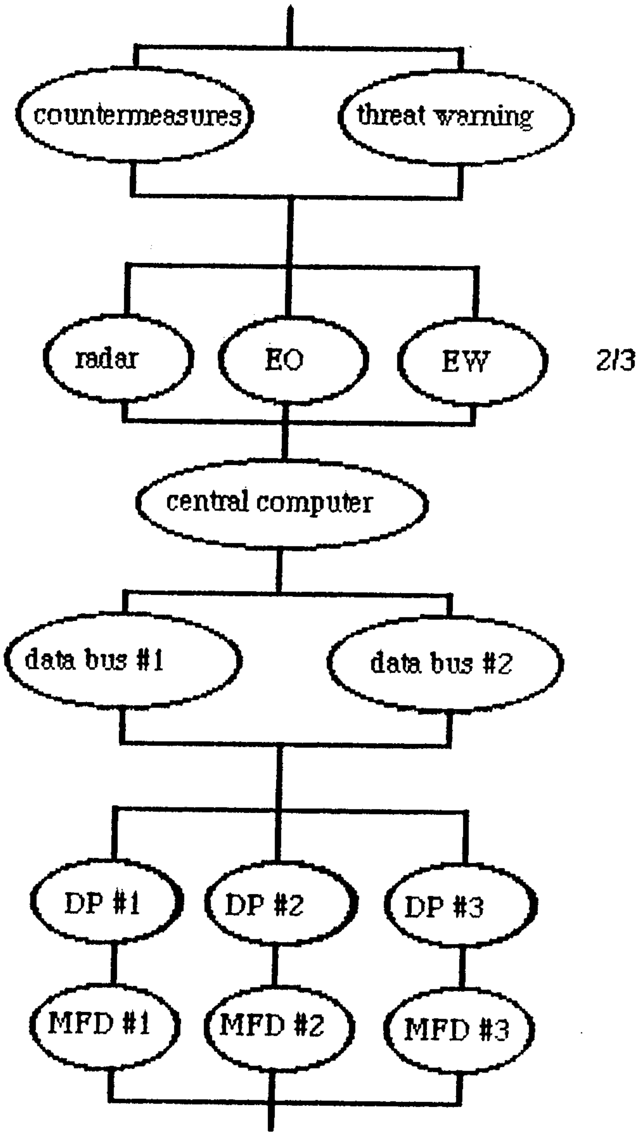

Figure 13, Tactical Sensor Systems (Mission Abort) Kill Tree

J. ARCHITECTURES

1. Federated

In a federated avionics system architecture, a moderate degree of control and coordination is handled by a central mission computer. The individual elements of the system usually have dedicated, independent data processors and are interconnected via data buses, typically via the MIL-STD-1553B. This degree of interconnectivity allows the system elements to work in cooperation and to share information, which is the major advantage of the federated system over the independent architecture. From a vulnerability standpoint, there are two weaknesses: 1) reliance on a central computer for control and coordination; and 2) reliance on shared data that is distributed via interconnecting data buses.

The key survivability issue for a federated system is to ensure uninterrupted and uncorrupted communications between the various avionics systems via the data bus or buses. Since the different systems are dependent upon a common data base, any break in this flow of data will cause system degradation. The exact nature of the degradation will be dependent upon the individual system function and the criticality of the data.

A critical component for a federated architecture is the central computer that functions to coordinate and control the various system elements. Unless a backup computer is available, this can represent a single point kill for the avionics system. With the central computer's functionality disabled, the interconnected systems may be unable to function independently.

Similarly, the data buses used to connect the system elements to the central computer are critical components. Disabling all of these data buses will serve to isolate the central computer and each individual system element from the rest of the system. This will prevent the essential flow of shared data and control signals, which is likely to result in the loss of much, if not all, of the functionality of the federated system. Figure 14 shows the critical components of the federated avionics architecture.

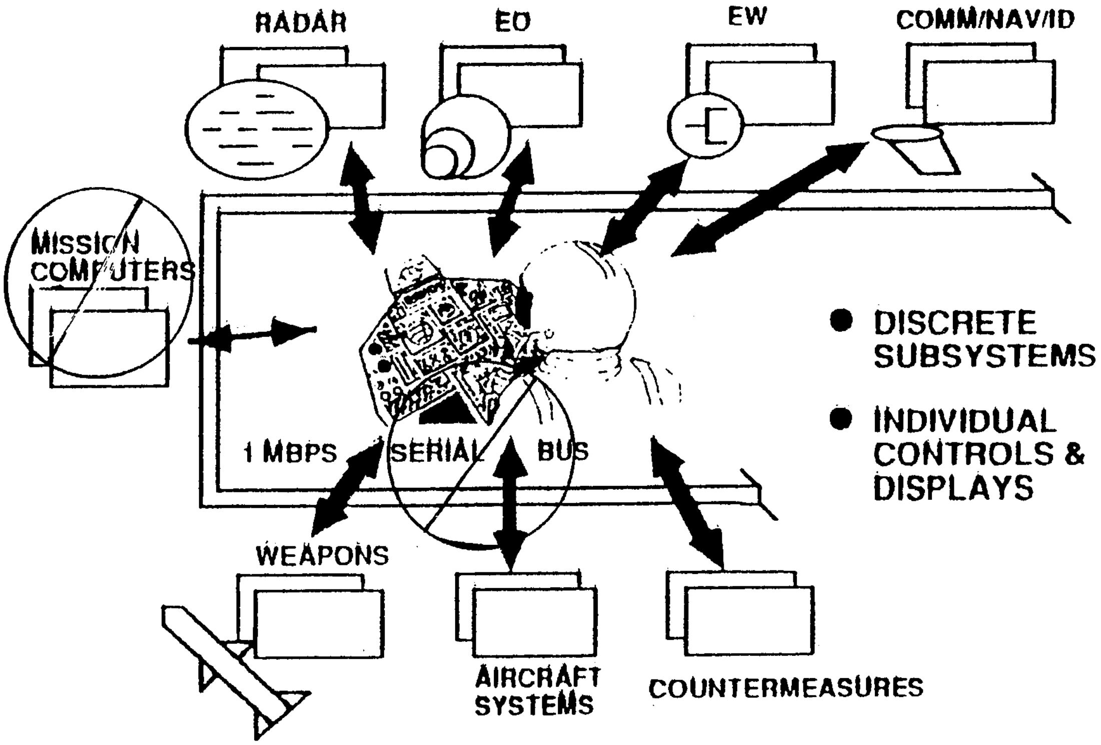

Figure 14, Federated Architecture Critical Components, After Ref. 1

2. Centralized

In a centralized avionics architecture, the main elements of the avionics system are packaged in standard modules which are located in one or more densely packed avionics racks. The system elements within the avionics racks are interconnected by means of high speed backplane buses, while connections to the various sensors and displays are made via both conventional and high speed data buses. Because the computer processing capabilities of the integrated architecture are centrally located and are shared among various elements, the data buses must be capable of handling a very high data rate. The centralized architecture makes extensive use of common modules and the sharing of the computer processors. To an even greater extent that the federated architecture, the survivability weaknesses of the centralized architecture are: 1) nearly total reliance on a central processor for data processing, control and coordination; 2) close proximity of critical components in a common avionics rack; and 3) reliance on data that is distributed via interconnecting data buses.

This architecture may have two major disadvantages in a combat environment: 1) it depends on many long data buses to collect and disseminate both data and command signals and 2) the loss of the single or co-located central computer(s) could result from a single hit. Since the other elements of a centralized system are largely dependent upon the central processing unit(s) for inputs, direction and coordination, loss of the central computer(s), or loss of communication with the central computer(s), could significantly degrade mission performance even to the extent of causing a kill of the aircraft.

A critical component for an centralized architecture is the central avionics rack that contains the processing modules which function to process data, coordinate and control the various system elements. Since the design co-locates the backup processors in the same or an adjacent avionics rack, this can represent a single point kill for the avionics system. With the centralized processing disabled, the centralized system may be unable to function unless some backup processing capability is provided in another location.

Similarly, the data buses used to connect the system elements to the central processors are critical components. Disabling these data buses will serve to isolate the central processors from the individual system elements. This will prevent the essential flow of data from the sensors to the processors and from the processors to the displays. Without a reliable data path, the functionality of the integrated system is likely to be compromised. Figure 15 shows the critical components of the centralized architecture.

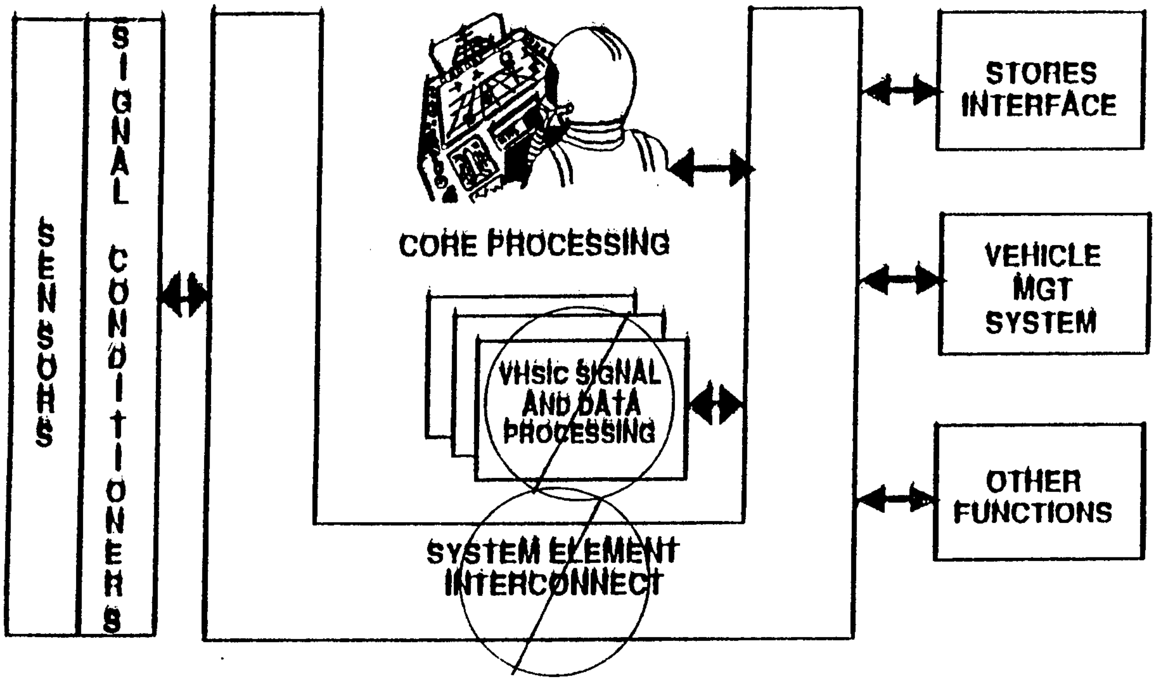

Figure 15, Centralized Architecture Critical Components, After Ref. 1

3. Distributed

The distributed architecture is similar to the integrated architecture in the use of common modules located in racks or cabinets. It different in that a significant amount of data processing is accomplished at the subsystem or element level. Rather than being located at a single, central location, the processors are distributed throughout the aircraft in nodes. A processor-intensive element, such as a radar or electronic warfare system, will typically incorporate a significant preprocessing capability at or near the antenna location. These processor nodes are interconnected via data buses, but are capable of some independent operation.

This architecture may enjoy several advantages in a combat environment, including: 1) less reliance on data buses; 2) intrinsic partitioning and 3) residual capability should communication with other system elements be interrupted [Ref. 1: p. 6].

Critical components for a integrated architecture are the avionics racks that contain the processing modules which function to process data, coordinate and control the various system elements. Since the design distributes these modules in nodes throughout the aircraft, a significant survivability advantage, there may be no single point kill for the avionics system, especially if the system can be dynamically reconfigured. With one or more of the processing nodes disabled, the distributed system may be able to continue to function, unless some essential capability is lost.

Similarly, the data buses used to interconnect the processor nodes located at the various system elements are critical components. Disabling these data buses will serve to isolate the distributed processors from the each other and their individual system elements. This will prevent the essential flow of data from the sensors to the processors and from the processors to the displays. Without a reliable data path, the functionality of the distributed system is likely to be compromised. In a similar manner as with the centralized architecture, redundant, physically separated data buses can be used in order to ensure a reliable data path for the system. Figure 16 shows the critical components for a distributed architecture.

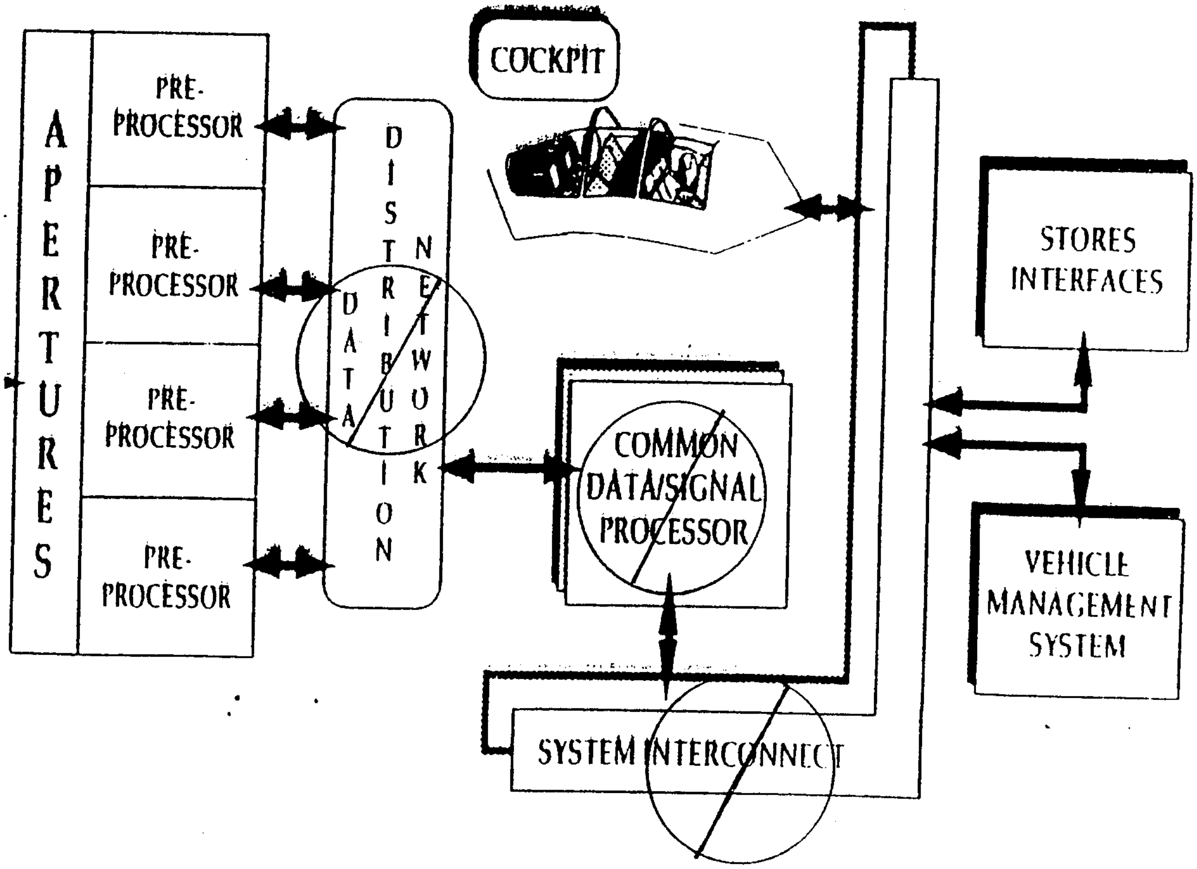

Figure 16, Distributed Architecture Critical Components, After Ref. 1

V. COMPUTING THE VULNERABLE AREA OF AVIONICS COMPONENTS

A. VULNERABILITY ASSESSMENT

As a part of the vulnerability assessment (VA) of the aircraft, it is necessary to:

- Select a kill category and level
- Assemble the aircraft technical and functional description
- Determine the critical components and their kill modes for the selected kill category and level
- Select the threat
- Determine the critical component kill criteria
- Compute the vulnerability measure for the selected threat and kill category and level

For the flight control systems, it is possible to conduct a VA assuming either an attrition or a mission abort kill. For the other systems, it is more probable that a mission abort kill will be appropriate for the VA.

The technical and functional descriptions are needed in order to identify the aircraft's critical components and to build a physical model of the component locations. Typically, a computer model of the aircraft that shows component locations is built using a computer aided design (CAD) software package. This model is then used to help determine the presented areas (Ap) of the components. In combination with the probability of killing a component given a hit on the component (Pk/h), the vulnerable area (Av) of a component can be determined [Ref. 3: p.158].

The vulnerable area of a given component is defined as the product of the presented area (Ap) in the plane normal to the approaching damage mechanism and the probability of kill of the component, given a hit on the component (Pk/h). In equation form: Av = (Ap)(Pk/h) [Ref. 3: p. 159]. Since it is extremely time consuming to compute the aircraft vulnerability manually, a number of computer programs have been developed for this task.

Two types of computer programs, shotline generators and vulnerable area routines, are typically used sequentially to conduct a vulnerability assessment of an aircraft to a single hit by a penetrator or fragment [Ref. 3: p.192]. The shotline generator programs usually model the exterior surface of the aircraft and its components with either surface patches or various geometric shapes. The program then superimposes a planar grid over the aircraft's surface from a particular direction and passes a set of parallel rays or shotlines through the aircraft, one shotline being randomly located in each grid cell. The shotlines are always normal to the grid plane and from the direction of the threat mechanism. The program traces the path of each shotline through the aircraft and specifies which components have been encountered along the shotline.

The vulnerable area routines, of which COVART is currently the state-of-the-art, are used to generate component and total aircraft vulnerable area tables for a single penetrator or fragment [Ref 3: p. 194]. The means by which this is accomplished is described as follows:

> "The component vulnerable area of each grid cell is the product of the cell presented area and the probability of component kill for the shotline in that cell. The vulnerable area of each component is the sum of the component vulnerable areas computed for each grid cell whose shotline passes through the component. The total aircraft vulnerable area is the sum of all the cell vulnerable areas, considering only the nonredundant critical components and any redundant critical component overlap." [Ref 3: p. 195]

Once the individual aircraft components' probability of kill given a hit, (Pk/h) and presented area (Ap) have been determined, the computer methods described can be used to estimate the overall vulnerability of the aircraft to a given threat. Because of their small size, avionics devices make a relatively minor contribution to the overall vulnerable area of a typical aircraft. Large vulnerable components such as fuel tanks, engines and the cockpit usually have a much greater vulnerable area to a given threat than the avionics system. However, although avionics devices are small, they are frequently critical components whose loss or damage could result in an attrition or mission abort kill. A kill in most avionics components will not usually result in an aircraft kill, but may lead to a mission abort. The decision on whether or not to abort must take into account the specific mission, threat and environmental conditions, since different missions have different levels of reliance on the avionics system [Ref. 16: p. 9].

There are two classes of critical components that generally make up the avionics system, the "black boxes" (more formally known as Line Replaceable Units or LRUs) and the wires or cables that interconnect them. Because of the nature of electronics devices, the impact of a projectile or fragments will usually either produce an immediate kill of the component (LRU, wire or cable) or the unit will survive [Ref. 16].

B. "BLACK BOX" VULNERABILITY

The design of a typical avionics "black box", or LRU, is specified in applicable civil or military standards. These standards establish the form factor, external design, mounting and environmental operating conditions for avionics components that are located in the avionics bay of an aircraft [Ref. 6: p.139]. Current standards include ARINC Specification 600 [Ref. 17], DOD-STD-1788 [Ref. 18] and MIL-M-28787 [Ref. 19]. Figure 6 shows the outline drawing of a DOD-STD-1788 LRU.

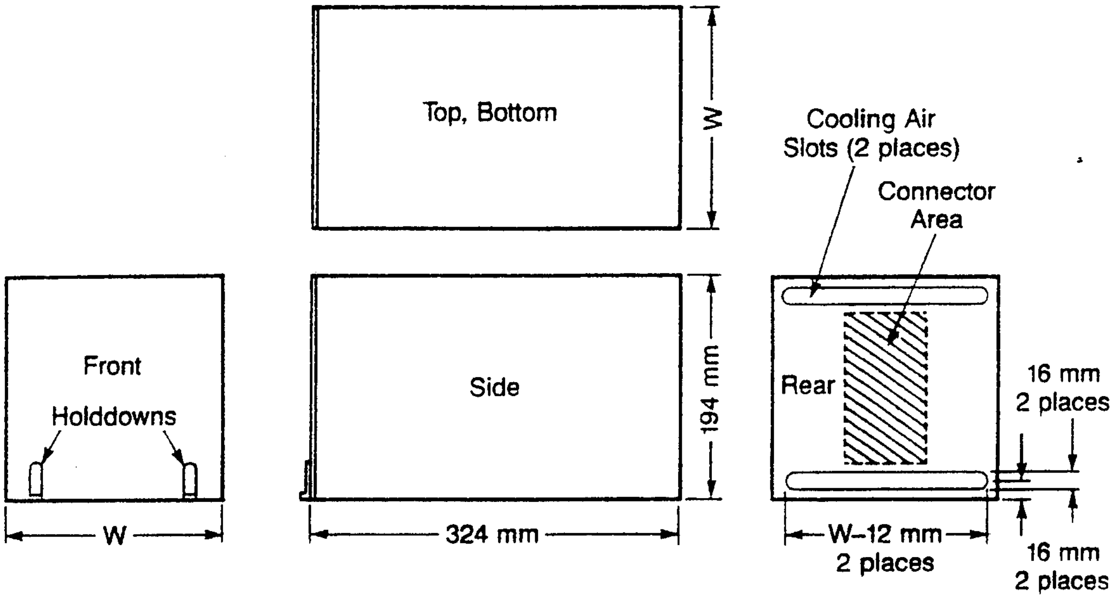

Figure 17, DOD-STD-1788 LRU (from Ref. 6)

The aircraft environment is typically described in precise, quantitative terms for the use of the avionics designer [Ref 6: p. 148]. The specified environment usually includes power, cooling and ambient air, pressure, temperature, vibration, shock, and the electromagnetic environment. This generally assumes a benign operating environment and does not typically specify the possible damage mechanisms that may be encountered by a tactical aircraft in a combat environment. The survivability requirements, such as ballistic tolerance to a given threat mechanism (e.g. 7.62 or

12.7 mm projectiles) is usually included in the overall aircraft specification since survivability is applicable to all systems, not just avionics.

For a given avionics component (LRU) to cease to perform its intended function as the result of a hit, the outer case must generally be penetrated by the damage mechanism (projectile or penetrator). This hole in the outer casing destroys the electromagnetic shielding and may compromise the forced air cooling system. Since LRUs are typically fairly densely packed with circuit cards and power supplies, the penetration into the interior of the LRU will cause a great deal of damage to these fragile assemblies. Internal health monitoring routines, such as built-in-test, are likely to identify the failure of multiple assemblies within the LRU as a result of the projectile or fragment damage. This will be likely to lead to a self-commanded shutdown of the component, unless this function is itself damaged. It is also possible that an electrical fault of sufficient magnitude to cause a fuse or circuit breaker to function will occur as a result of the hit, thereby cutting off power to the LRU. The kill of an electronics component after a hit by a projectile or fragment is likely to be immediate (less than one second) [Ref. 16: p. 10].

In the case of an explosive warhead, such as a 23mm HEI round, the effects on the LRU are devastating. Internal circuit card assemblies are temperature sensitive and the heat of the explosion is very likely to destroy the items located in the interior of the LRU. The probability of kill for such a warhead is likely to approach unity.

C. CABLE VULNERABILITY

Since avionics components are typically connected via cables or wires, the vulnerability of these cables and wires to damage by projectiles and fragments is a significant concern. Recent testing under the sponsorship of the Air Force [Ref: 20] has provided a great deal of information about the effects of projectile and fragment damage on wire bundles and cables. A major reason for concern about these effects is that damage to cables and wire bundles is difficult to locate and repair. While circuit breakers and fuses can be expected to protect the various avionics components, shorting to ground and arcing can be expected to result from the impact of a damage mechanism (projectile or fragment) on the wires or cable [Ref 20: p. 1]. In addition to disabling the power, control or signal path, the current carried by the severed cable presents a possible source of ignition for secondary fires or explosions.

When computing the vulnerable area of the aircraft, the contributions of the cables and wire bundles must be included since the loss of power or signals to a critical component is essentially equivalent to the loss of the component itself. While small in diameter, many wire bundles and cables have a large presented area because of their length. Most shotline generator computer programs conclude that a cable or wire is damaged by a projectile or fragment only if the centerline of the projectile or fragment passes through the cable or wire. This can lead to an underestimation of the vulnerable area, since penetration of the outer shielding that exposes the conductors is sufficient to cause damage and in many cases it is not necessary to completely sever the cable or wire to have damage occur. This effect is shown in Figure 18. Flint

[Ref. 20] proposes that a radius addition be added to all wire bundles and cables in order to compensate for the shotline methodology currently in use. This would increase the probability of a hit being recorded on a given cable or wire bundle and would correct for the currently understated number of hits that results from the shotline methodology in use. This should result in an increased presented area and a corresponding increase in vulnerable area a result of the contribution of the cables and wire bundles to the avionics system vulnerable area.

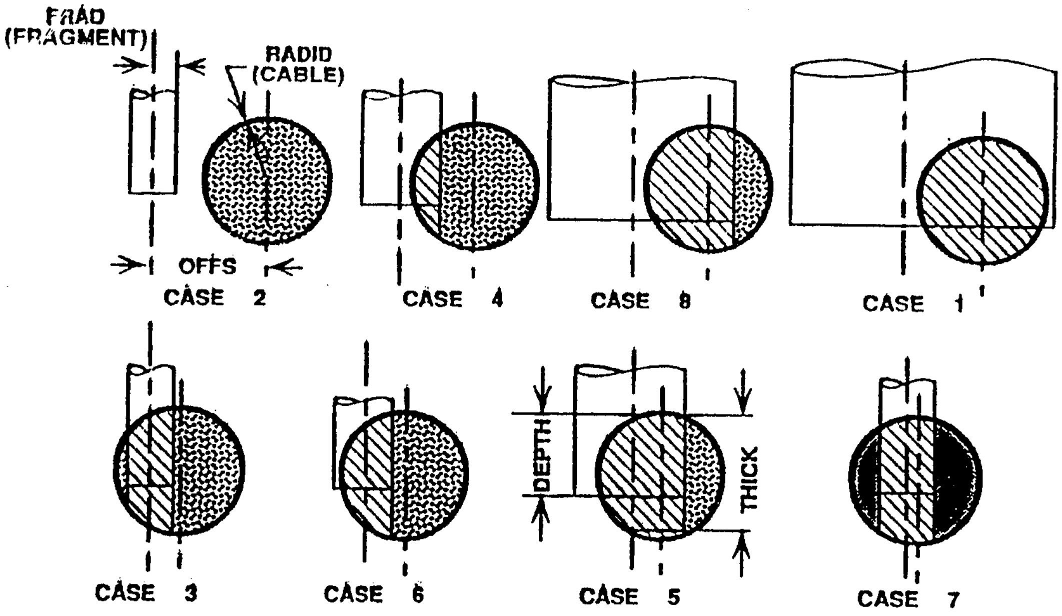

Figure 18. Effects of Fragment Size and Offset (from Ref.20)

VI. VULNERABILITY REDUCTION IN AVIONICS DESIGN

Digital avionics systems can contribute positively to the survivability of a tactical aircraft in many ways, including reducing the susceptibility of the aircraft (making the aircraft harder to hit) and reducing the vulnerability of the aircraft (making it harder to kill, if hit). Susceptibility factors were covered in Chapter III. Chapter IV discussed vulnerability effects for the most common types of avionics systems, with the exception of computer systems. Since the computer systems are of critical importance to all of the other avionics systems (e.g flight control systems, engine control systems, flight avionics systems and tactical sensor systems), the computer systems were not treated separately. The following chapter presents the six vulnerability reduction concepts as applicable to avionics systems.

A. VULNERABILITY REDUCTION CONCEPTS

Vulnerability reduction is defined as the use of any design technique or equipment to control or reduce the amount of damage or the consequences of damage to the aircraft, when the aircraft is hit by one or more damage mechanisms [Ref. 3]. The six vulnerability reduction concepts are [Ref. 3]:

- Component Redundancy (with separation)
- Component Location
- Passive Damage Suppression
- Active Damage Suppression
- Component Shielding
- Component Elimination

Each of these vulnerability reduction concepts may used to improve the survivability of the avionics systems.

1. Component Redundancy (With Separation)

Component redundancy refers to the use of multiple devices, parts or mechanisms to perform a given task [Ref 3]. Systems may be designed with total redundancy or only partial redundancy. A choice also exists between actual redundancy, using identical devices, parts or mechanisms, or functional redundancy only. The use of multiple, redundant data buses in parallel is an example of actual redundancy using identical components. The requirement for physical separation of the redundant devices, parts or mechanisms is intended to prevent the redundant items from being killed by a single event. For example, it would be considered good design practice to route the multiple redundant data buses as far apart from one another as possible, within the constraints of the aircraft structure. When the data buses are routed on opposite sides, damage to one side of the aircraft alone would be unlikely to result in loss of all data bus functionality.

2. Component Location

Component location means the choice in the design phase to position a component such that a damage mechanism is less likely to kill the component [Ref. 3]. Good design techniques applicable to improved survivability of avionics devices include:

- Orienting a component's presented area to reduce the likelihood of being hit by a damage mechanism coming from the most probable direction.
- Locating noncritical or ballistically hardened components in front of more vulnerable components.

- Reducing the presented area of non-redundant components.

- Locating components in order to prevent cascading damage.

In the case of a ground attack aircraft tasked with close air support, it would be good design practice to avoid locating critical components near the bottom of the aircraft, since this is the direction where the majority of damage mechanisms are likely to be coming from. For aircraft that use a central avionics bay, the demands for easy access for maintenance must be traded off with the need for survivability in locating the critical avionics components. For most aircraft, the trend towards component miniaturization aids aircraft survivability by reducing the presented area of critical components, thereby reducing the aircraft's vulnerable area.

3. Passive Damage Suppression

Passive damage suppression refers to features that either contain the damage or reduce the effects of the damage when an aircraft encounters a damage mechanism [Ref. 3]. Good design techniques applicable to improved survivability of avionics devices include:

- Damage Tolerance

- Ballistic Resistance

- Delayed Failure

- Fire and Explosion Suppression

- Fail-Safe Response

Most avionics components are composed of printed circuit cards and their associated power supply and backplane, located in a housing ("black box") that functions as an environmental shield from dust, water, and electromagnetic interference and provides a channel for cooling air. The "black box" is typically optimized for light weight and small size, with ballistic resistance rarely being a consideration. Vulnerability reduction techniques available to the avionics designer include the use of materials that are tolerant of the loss of the integrity of the environmental shield that is the component housing. The key passive damage suppression technique for avionics is to ensure that components are able to be easily isolated via circuit breakers, preventing a "cascade" failure to the system.

4. Active Damage Suppression

Active damage suppression is a technique that employs a sensor or other device to sense the onset of a damage process and activates some mechanism that contains the damage or reduces its effects [Ref.3]. The chief example of this type of technique is a fire detection and extinguishing system. Since avionics devices are generally very sensitive to damage by fire or overheating, the use of fire suppression devices in avionics bays could improve their survivability.

5. Component Shielding

Component shielding refers to the technique of using coatings or materials that resist or absorb the damage mechanisms [Ref. 3]. The use of armor is the most common example of this technique. Here the design tradeoff is between the weight of the shielding and the necessary level of ballistic tolerance. Since most avionics devices are not themselves in hardened housings, this technique is usually applicable to shielding around the avionics bay. To save weight, the shielding is usually installed in only the most probable direction for the given damage mechanism.

6. Component Elimination

Component elimination refers to the design choice of either eliminating a component entirely or replacing it with another, less vulnerable, component [Ref. 3]. An example for an avionics component would be to choose a passively cooled component over one which relies on forced air cooling, since this reduces the component's vulnerability to damage should cooling air supplies be lost.

B. CHOICE OF AVIONICS ARCHITECTURE

The avionics designer has a choice of three main avionics architectures: federated, centralized and distributed. Each is highly dependent upon the uninterrupted flow of data via the digital data buses and on computer processing capability. The vulnerability reduction concepts applicable to each architecture are discussed below.

1. Federated

The federated system can be designed to be more survivable by providing physically separated backup data paths using multiple redundant data buses with backup bus controllers and a backup central computer. The use of multiple, interconnected data buses, each of which is dedicated to a particular function, can provide a degree of compartmentalization. The physical placement of the data bus cables should be as widely separated as possible, within the constraints of the aircraft design. The goal is to assure the reliable transmission of data between the various remote terminals in the system in order to maintain system integrity and functionality.

2. Centralized

The centralized system can be designed to be more survivable by providing backup data paths using multiple redundant data buses, either with backup bus controllers or by using newer data bus designs that do not rely on bus controllers. The physical placement of the data bus cables should be as widely separated as possible, within the constraints of the aircraft design, but all must converge at the central avionics rack(s). The use of a centralized, integrated processing capability means that it is nearly impossible to duplicate this capability in a physically separate location. Hence, the central processing and data distribution systems must be protected from damage in order to ensure survivability of the system. Hardening and/or shielding of the co-located group of critical components is the most likely vulnerability reduction concept to be effective without compromising the economic advantages of the centralized architecture.

3. Distributed

From a survivability perspective, it can be argued that the distributed architecture is preferable because damage at any single site should be unable to disable all systems. The remaining processing capability may be sufficient to enable a degree of system functionality even after some damage has been inflicted. Still, the information that is shared over the data buses could be interrupted due to damage, even if individual systems are capable of functioning. The impact of interrupting the data flow would be likely to impede continued system operation, making the availability of redundant data paths an essential consideration for a distributed architecture, just as it is for the federated and centralized architectures.

VII. CONCLUSIONS

In the design of a modern tactical aircraft, which is highly dependent upon digital avionics systems for its mission performance, attention should be paid to the survivability of the avionics systems when the aircraft is operated in a man-made hostile environment. The traditional considerations of reliability, fault tolerance and component redundancy that take into account known or anticipated failure modes of the avionics systems should be augmented by consideration of the catastrophic effects of combat damage.

For most common combat threats, damage to the avionics system is more likely to result in a mission abort kill than an attrition (loss of aircraft) kill. However, an unstable fly-by-wire aircraft could be attrited if the damage is sufficient to disable the flight control system. There may be an interesting parallel in the design of some fly-by-wire systems to the hydraulic system design that was typically used in the 1960s. At that time, all of the hydraulic systems were generally routed to each of the servo actuators. In combat, this proved to be undesirable in that a single massive hit to the servo area could knock out all of the aircraft hydraulic systems simultaneously. In some fly-by-wire designs, all of the data buses used to send flight control commands to the servos are likewise connected to each servo. It is possible that a single massive hit to the servo area could sever all of the data bus cables and disable all of the flight control data streams simultaneously, resulting in loss of control. Another possible single point failure is the flight control computer in an unstable aircraft. In some aircraft designs, the central flight control computer has such a major role in the flight control system that a disabling hit to this component will result in the loss of control, regardless of pilot input.

The majority of possible kill modes of avionics components will lead to a mission abort kill. The decision on whether or not to abort must take into account the specific mission, threat and environmental conditions, since different missions have different levels of reliance on the avionics system. As modern tactical aircraft become increasingly reliant on their avionics systems, the contribution of these systems to the vulnerability of the aircraft is likely to increase.

It is probable that as more combat data is available, the survivability effects of digital avionics systems will be better understood. For now, the fact that avionics systems represent 30-40 percent of the aircraft fly-away costs, although only 5-6 percent by weight, dictates that a cautious approach to the effects of digital avionics systems on the survivability of modern tactical aircraft be pursued.

LIST OF REFERENCES

[Citation by number:]

1. Naval Air Systems Command, Avionics Systems Engineering Division, AIR-546, Advanced Avionics Architecture and Technology Review - Final Report, 6 August 1993.

2. Naval Air Systems Command, Avionics Systems Engineering Division, AIR-546, Rising Avionics Costs as a Percent of the Total Weapons System, 20 September 1992.

3. Ball, Robert E., The Fundamentals of Aircraft Combat Survivability Analysis and Design, 1985.

4. Joint Services Safety Conference, System Safety Panel, Guide For Evaluating Hazard Analysis, Technical Report JSSC-TR-4, March 1991.

5. Joint Technical Coordinating Group for Munitions Effectiveness, Aerial Target Vulnerability Working Group, COVART 3.0 - A Simulation Program For Computation of Vulnerable Areas and Repair Times - User Manual, 61 JTCG/ME-91-3, January 1993.

6. Spitzer, Cary, Digital Avionics Systems, Principles and Practices, Second Edition, 1993.

7. MIL-STD-704E: Aircraft Electrical Power Characteristics, May 1991.

8. RTCA DO-160C: Environmental Conditions and Test Procedures for Airborne Equipment, Radio Technical Commission for Aeronautics, Inc., 1989.

9. MIL-STD-1553B: Digital Time Division Command/Response Multiplex Data Bus, Notice 2, September 1986.

10. DOD-STD-1773: Fiber Optics Mechanization of an Aircraft Internal Time Division Command/Response Multiplex Data Bus, Notice 1, October 1989.

11. Aerospace Standard AS4704.1: Linear Token Passing Multiplex Data Bus, Society of Automotive Engineers, 1988.

12. ARINC Specification 429: Mark 33 Digital Information Transfer System, Aeronautical Radio, Inc., 1977.

13. ARINC Characteristic 629: Multi-Transmitter Data Bus, Aeronautical Radio, Inc., November 1989.

14. Aviation Week & Space Technology, F-16 Shoots HARM with EA-6B Support, 17 Oct 1994.

15. Ahrens, Roger A., et al, Survivability Assessment Guidelines For Flight Control Systems, Technical Report AFFDL-TR-74-39 Volume I, Air Force Dynamics Laboratory, Air Force Systems Command, Wright-Patterson AFB, OH, June 1974.

16. Pullen, Keats, A., Effects of Redundancy on Survival of Critical Avionics Equipment, USA Ballistic Research Laboratories, Aberdeen Proving Ground, MD, BRL Memorandum Report No. 2266, January 1973.

17. ARINC Specification 600, Air Transport Avionics Equipment Interface.

18. DOD-STD-1788, Avionics Interface Design Standard, 15 May 1988.

19. MIL-M-28787, Modules, Standard Electronic, General Specification for, 30 March 1989.

20. Flint, James B., Submunition Evaluation Program Project CHICKEN LITTLE: The Vulnerability of Wire Cable and Wire Bundles to Fragment Attack, Department of the Air Force, Air Force Development Test Center, Eglin AFB, FL, April 1994.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center....................2
Cameron Station
Alexandria, Virginia 22304-6145

2. Library, Code 52...2
Naval Postgraduate School
Monterey, California 93943-5101

3. Distinguished Professor Robert E. Ball, Code AA/Ba......1
Department of Aeronautics and Astronautics
Naval Postgraduate School
699 Dyer Road, Room 137
Monterey, California 93943-5107

4. Professor Daniel J. Collins, Chairman, Code AA/Co.......1
Department of Aeronautics and Astronautics
Naval Postgraduate School
699 Dyer Road, Room 137
Monterey, California 93943-5107

5. Aerospace Engineering Curricular Officer, Code 31.......1
Department of Aeronautics and Astronautics
Naval Postgraduate School
699 Dyer Road, Room 133
Monterey, California 93943-5107

6. Naval Air Systems Command, Code AIR-4.5.................1
Naval Air Systems Command Headquarters
1421 Jefferson Davis Highway
Arlington, Virginia 22243-5000